STATE BEHAVIOR IN CYBERSPACE:
RUSSIA, CHINA and the U.S.

AYNABAT GARAYEVA
113605016

ISTANBUL BILGI UNIVERSITY
FACULTY OF ECONOMICS AND ADMINISTRATIVE SCIENCES
DEPARTMENT OF INTERNATIONAL RELATIONS

In Partial Fulfillment of the Requirements for the Degree
Master of Arts
International Relations

Academic Advisor: Assist. Prof. Mehmet Ali Tuğtan
Submitted: 03/12/2014

State behavior in cyberspace: Russia, China and the U.S.

Siber alanda devlet davranışları:
Rusya, Çin ve ABD

Aynabat Garayeva
113605016

Tez Danışmanı: *Assist. Prof.* Mehmet Ali Tuğtan
Jüri Üyesi: *Assoc. Prof. Doc.* Yaprak Gürsoy
Jüri Üyesi: *Assist. Prof.* Okan Tanşu

Tezin Onaylandığı Tarih: 24.12.2014

Toplam Sayfa Sayısı: 73

Anahtar Kelimeler (Türkçe):
1) Siber alan
2) Uluslararası normlar
3) Siber tehdit
4) Güvenlik
5) Ihlal

Anahtar Kelimeler (İngilizce):
1) Cyberspace
2) International norms
3) Cyber threat
4) Security
5) Infringement

Abstract

This study investigates why and how nation-states infringe on international norms of state behavior in cyberspace. The research has discovered that nation-states with high cyber capabilities are more likely to benefit from anonymity and interconnectivity of this virtual domain to exercise their power internationally by arbitrarily interfering with internationally interconnected infrastructure or using any type of information control techniques. On the contrary, countries with low cyber capabilities prefer to survive in such borderless and competitive domain by denying, disrupting, manipulating their citizens' access to the internet or other networked technologies. Moreover, all cases of norm infringement in a virtual domain are directly related to the political conflicts in reality. If this virtual domain became another arena for warfare then this is not because of its ubiquitous or anonymous feature, this is what states make of it.

Özet

Bu çalışma ulus-devletlerin siber alanda uluslararası devlet davranışları normlarını neden ve nasıl çiğnediğini araştırmaktadır. Bu araştırma yüksek siber yeteneklere sahip olan ulus-devletleri, herhangi bir bilgi kontrol tekniği veya bunun gibi görsel domainlerin anonimliğini ve birbiri ile bağlanabilirliğinden dolayı keyfi olarak karışıklığa sebebiyet vererek uluslararası güç denemesi yaptıklarından daha çok fayda sağlamaktadırlar. Öbür taraftan, düşük siber yeteneklere sahip ülkeler bu tür sınırsız ve rekabetçi domainlere karşı kurtluşu ancak inkar, bozma, manupilasyon ile vatandaşlarının bu tür internet ve network teknolojilerine girişini engellemekte aramaktadır. Bu görsel domain savaş hali için başka bir arena olabilirdi ama bu mümkün değil, çünkü onun anonim özelliği var, bu ise ulus-devletlerin istediğidir.

ABBRIVATIONS

ACT	Agile Cyber Technologies
AFRL	Air Force Research Laboratory
APT	Advanced Persistent Threat
BART	Bay Area Rapid Transit System
BBC	British Broadcasting Corporation
CASIC	China Aerospace Science and Industry Corporation
C&C	Command-and-Control
CENTCOM	Central Command
CERT	Computer Emergency Response Team
CFECIE	Congress on Foreign Economic Collection and Industrial Espionage
CIA	Central Intelligence Agency
CIIS	Convention on International Information Security
CSSG	Cyber Security Strategy for Germany
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
FBI	Federal Bureau of Investigation
GBP	Great Britain Pound
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
IP	Internet Protocol
ISP	Internet Service Provider
ISC	International Strategy for Cyberspace
IT	Information Technology
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
NGO	Non-governmental Organization
NSA	National Security Agency
ONI	OpenNet Initiative
PLAN	People's Liberation Army Navy

RBN	Russian Business Network
RSA	American computer and network security company
SCADA	Supervisory Control and Data Acquisition
SIGINT	Signals Intelligence
U.K.	United Kingdom
UN	United Nations
UNIDIR	United Nations Institute for Disarmament Research
U.S./U.S.A.	United States/United States of America
USD	United States Dollar
USB	Universal Serial Bus
USSR	Union of Soviet Socialist Republics

Table of Contents

INTRODUCTION

Despite growing security disputes in cyberspace, nation-states have yet to completely determine their behavior in this vast and borderless domain. In fact, states are and will continue to be important actors, but the borderless state of cyberspace makes it an attractive domain for both nation-states and non-state actors alike to manifest their power. Some cyberspace security experts (Tikk 2010; Betz and Stevens 2011) claim that 'the lack of direct evidence of the attacking entity's identity – that may make such 'grey area' attacks even more attractive' (Tikk et al. 2010, p. 103). Recent discussions on cyberspace espionage conducted by the White House, such as the case revealed by former National Security agent Edward Snowden, demonstrate once again how nation-states utilize cyberspace for their benefit by infringing on international norms. In fact, according to Harris (2013), it was U.S. officials in the role as cyberspace hegemon who blamed other governments such as Russia and China in cyber-attacks:

> *The Obama administration has singled out China and Russia as "aggressive" players in the world of cyber-espionage and warned that they will continue to try and steal US industrial and technological secrets.*

Such aggressive behavior of nation-states towards each other causes an imbalance not just in the virtual environment but in the international system as well. Thus, due to security reasons governments have now started to reshape and constrain access to information, freedom of speech, and other elements of cyberspace within their territory. Recent scholarship has shown how governments are moving to use the rapidly-developing technologies for cyberspace controls and regulation. Ronald J. Deibert, director of the Canada Centre for Global Security Studies and the Citizen Lab, provides invaluable data on internet censorship as well as documenting and analyzing internet filtering practices in over three dozen countries.

This study investigates the role nation-states play in cyberspace and the way in which their cyberspace behavior impacts real life. A bulk of the research lays claim that international disputes over cyberspace security have occurred due to the borderless state of this domain and the anonymity of the attacking entity. Unfortunately, those studies have skipped the most important aspect which emphasize that 'the social relations always begin and end outside cyberspace, even if their mediation is performed through a complex of machine actors ...' (Betz and Stevens 2011, p. 41). Deibert (2012) claims that the increasingly dynamic competition among states for influence in and through cyberspace is manifested in the creation of dedicated cyber armed forces and an arms race in cyberspace. This assertion is based on cyberspace security experts and scholarly arguments, case studies, and reports on cyberspace security analyzing how nation-states themselves create mistrust and anarchy in this virtual domain in order to demonstrate their power. The research investigates why and how nation-states infringe on international norms of state behavior in cyberspace. Based on Wendt's theory of anarchy, I explain that the behavior of states in cyberspace is determined by their interests rather than by the borderless feature of this virtual domain.

This thesis is divided into the following six sections: the introduction, 'The New Domain of the International System', 'Power Politics and Cyberspace', 'Nation-States in Cyberspace', 'Findings', and the conclusion. The introduction provides the general idea regarding the research topic and some scholarly arguments related to the research question. The first chapter is entitled 'The New Domain of the International System' and discusses the various determinants of the concept of 'cyberspace', who is considered a cyberspace actor, and also points out some of the challenges, risks, and threats posed by cyberspace. The second chapter is called 'Power Politics and Cyberspace' and includes theoretical frameworks of power politics from different

perspectives, namely neo-realist, neo-liberal, and constructivism, and explains the type of power politics applicable to cyberspace. Moreover, it discusses the 'security dilemma' in the virtual domain. The third chapter 'Nation-States in Cyberspace' continues to consider the roles of nation-states in cyberspace by conducting a deep research on their behavior in the fifth domain and points out the types of international norms they are more likely to infringe upon in order to manifest their power. The fourth chapter is entitled 'Findings' discusses the results of the research, which states that disagreements on cybersecurity cooperation as well as the development of offensive or defensive cyberwarfare capabilities both create mistrust and competitiveness in the international system which, in turn, decrease the cybersecurity of others. The conclusion then provides final remarks and discusses future steps that should be taken towards building security in cyberspace.

METHODOLOGY

The purpose of this research is to explore and explain how and why nation-states infringe upon international norms of state behavior in cyberspace. During the data collection process, I used a stratified sampling technique as I already knew I was going to concentrate specifically on Russia, China, and the U.S. Accordingly, the primary units of analysis of this inquiry are nation-states.

The research design is content analysis based on case studies, reports, cyberspace security strategies, newsletter articles, research articles and books, as well as existing statistics provided by the OpenNet Initiative (ONI) database. By using cyberspace security reports and case studies provided by the NATO Multimedia Library and existing data on internet censorship provided by the ONI database, this thesis examines the behavior of the aforementioned states in cyberspace.

Content analysis is one of three types of unobtrusive research methods, which is an appropriate method in studying social behavior without affecting it. Content analysis well suits to study communications and to answering the classic question of research in communications, which is 'who says what, to whom, why, how and with what effect?' (Babbie 2007, p. 320). Another advantage of this type of research design is that it allows for the correction of errors without the need to repeat the whole research project. In regard to this project, state behavior is an interchangeable quality. If anything changes regarding to the behavior of any state, I can add it to the content without affecting to the result of prior research.

Another research method I used is analyzing existing statistics, which is a second type of unobtrusive research. Existing statistics are previously collected data that has been analyzed in at least one way. The two primary ways a researcher can collect existing research are prior research and social programs. In this project, I used prior research conducted by ONI to identify and document internet filtering and surveillance methods to analyze state behavior in cyberspace. In fact the 'existing data do not cover exactly what we are interested in, and our measurements may not be altogether valid representations of the variables and concepts we want to make conclusions about' (Babbie 2007, p. 333). Accordingly, in this research, the limitation posed by ONI data was that not all states were tested on internet censorship and surveillance at the same period of time. For instance, Russia was tested in 2010, China in 2011, and the U.S. in 2009, which, in turn, means that the behavior of target states at the same period of time is unclear. In fact, any type of unobtrusive research methods can raise problems of validity and reliability but can be handled through logical reasoning and replication.

CHAPTER 1

THE NEW DOMAIN OF THE INTERNATIONAL SYSTEM

Despite being different from other domains in several respects, cyberspace is accepted as the fifth strategic domain with the other four other domains being land, sea, air, and space. The most important difference of this domain is it is entirely manmade. Its artificiality creates a problem of defining the cyber domain and its relevance to politics. This issue can be further discussed from both technical and political aspects. At a technical level, 'cyberspace is a network, a platform for new technological innovations such as social media, a conduit for communication, and a repository of information' (Reardon 2012, p. 26). In fact, this domain is conceptually connected to various types of technologies and technological innovations such as the internet, information technology, communication technology, networks, etc… Accordingly, determining the boundaries between cyberspace, its related practices and technical standards, and the individual users that constitute networks have become among the main concerns of scholars and policy makers.

From a political aspect, Betz and Stevens (2011) argue that there is a debatable issue on determining the operations of cyber-power and the actors which cyberspace may empower in different ways and to different degrees under various conditions. A wide range of actors such as individuals, governmental and non-governmental organizations, terrorists and insurgents, multilateral global institutions and media conglomerates, etc... 'seek to use cyberspace to pursue its own ends, whether these be individually or in concert with others' (Betz and Stevens 2011, p. 39). Reardon and Choucri (2012) claim that potentially dangerous networks of non-state actors can be treated as a threat to the security of the state as well as its citizens.

1.1 What is CYBERSPACE?

The concept of ‘cyberspace’ doesn’t have a standard definition like other technology terms. Rather, it describes the virtual world of computers, with the advent of the internet, cyberspace took the global form of network of computers.

The word "cyberspace" is credited to William Gibson, who used it in his 1984 book *Neuromancer*. Gibson defines cyberspace as ‘a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity’ (p. 128). Today, the concept of cyberspace has several definitions both in scientific literature and in official governmental documents. Even though it has been declared as a new domain, “cyberspace” has yet to have a fully agreed-upon official definition. Accordingly, I will refer to some of these definitions in this study in order to cover all aspects of this new virtual environment.

The first speaker of the BBC program and series producer of *The Net*, Stephen Arkell, introduced the concept of ‘cyberspace’ in a comprehensive way for people who were unfamiliar with communicating on the internet. It is a computer system that allows almost instantaneous linkage with users around the world and access to bulletin board information ranging from politics to recipes.

Myriam Dunn Cavelty (2007) compared ‘cyberspace’ to an ocean where information flows to-and-from freely and the shortest distance between any two points isn’t a straight line at all as the points are instantly connected by the flows. Yet each node on the internet has always

been linked with a specific internet protocol (IP) address, which in turn corresponds to a specific computer in a particular location. These IP addresses have long been organized into national domains (p. 68).

Cybertheorist Allucquere Rosanne Stone (1991) defines cyberspace as 'incontrovertibly social spaces in which people still meet face-to-face, but under new definitions of both 'meet' and 'face''. In other words, despite the lack of physical geography, cyberspace offers opportunities for the creation of collective communities and individual identities. According to Stang (2013), cyberspace differs from the other commons domains, because it is not a *physical* domain and due to the private sector's preponderant role in both the infrastructure and the management of the domain. All of the physical nodes of the internet also exist within states and are subject to national law, rather than existing physically outside of national control as for the other commons (p. 3).

Despite all this, cyberspace is accepted as a global commons its supposed lack of borders is best seen as a wish rather than a feature. J. Lewis (2010) points out that the concept of cyberspace undercuts both national and international security and is increasingly unsustainable as other governments seek technological and policy solutions to extend their control in this domain. But the policies that grew from this wish now face challenges in the new conditions of the twenty-first century, in which the internet is no longer a U.S. artifact, but rather an arena in which states contend (p. 56). In fact, today's cyberspace is no longer science fiction, instead another strategic domain.

Within the military, cyberspace has been identified as a new fifth arena, in addition to land, sea, air and space, in which military operations can be performed. Operations conducted

within cyberspace are called cyberspace operations. Such operations may be both offensive and defensive and performed independently or as a complement to conventional warfare.

In this study, according to the U.S. Department of Defense (DoD), the concept of cyberspace refers to 'a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers' (DoD 2010, p. 86).

The growing importance of cyberspace in modern society increases its use for international disputes. Its role on the international arena as an efficient medium for protest, crime, espionage and military aggression makes it an attractive domain for nation-states as well as non-state actors in cyber conflicts. While we try to understand the implications of this new domain, we shouldn't forget to discuss and determine the cyberspace actors.

1.2 Who are they – CYBERSPACE ACTORS?

More and more people are getting online as each day passes. Cyberspace is becoming a place where individuals and communities are socializing and organizing themselves across national borders and traditional sociocultural boundaries. Besides connecting hundreds of people and communities in one 'space', cyberspace has also brought several new threats to that society. In fact, cyber dependency has rapidly spread in our society and complex interconnections between various sectors have increased the vulnerability of attacks against both civilian and military infrastructures.

Although the nation-states play the main role in managing and monitoring this virtual domain, there are non-state actors that exercise their power independently to challenge states in

cyberspace. Katharina Ziolkowski (2013) explains the emergence of many groups of non-state actors in cyberspace by pointing to the particular challenge of the anonymity of who perpetrated malicious actions and the difficulty in tracking those actions back to their sources. Andrew Hoskins and Ben O'Loughlin (2010) also claim that in the new media ecology, nobody knows who will see an event, where and when they will see it, or how they will interpret it. It, in turn, may explain that the effects of power in a new domain may be as unintended as they are intended. The case of the CIA-Saudi site in 2008 explicitly illustrates how the unintended causalities of power has been exercised irresponsibly and caused collateral damage. As a result of US military actions against extremists planning attacks on American forces in Iraq, more than 300 servers in Saudi Arabia, Germany, and Texas were disrupted (Nakashima 2010).

1.2.1 Non-State Actors in Cyberspace

The borderless and even lawless network of interconnected networks have caused an emergence of a range of non-state actors such as hackers, (organized) cyber criminals, hacktivists[1], cyber terrorists, and also the private sector, NGOs, etc. Scholars (Farivar 2009; Czosseck and Geers 2007) state that there is no clear-cut distinction between these actors as they have globally different definitions and legal frameworks. Moreover, political agendas and the media determine the assessments of the same action differently and show their own classification of events.

[1] Hacktivism is an artificial word composed of the terms activism and hacking, and is said to be originally coined by *Omega*, a member of Cult of the Dead Cow hacker collective in 1996, describing it as 'the use of legal and/or illegal digital tools in pursuit of political ends'.

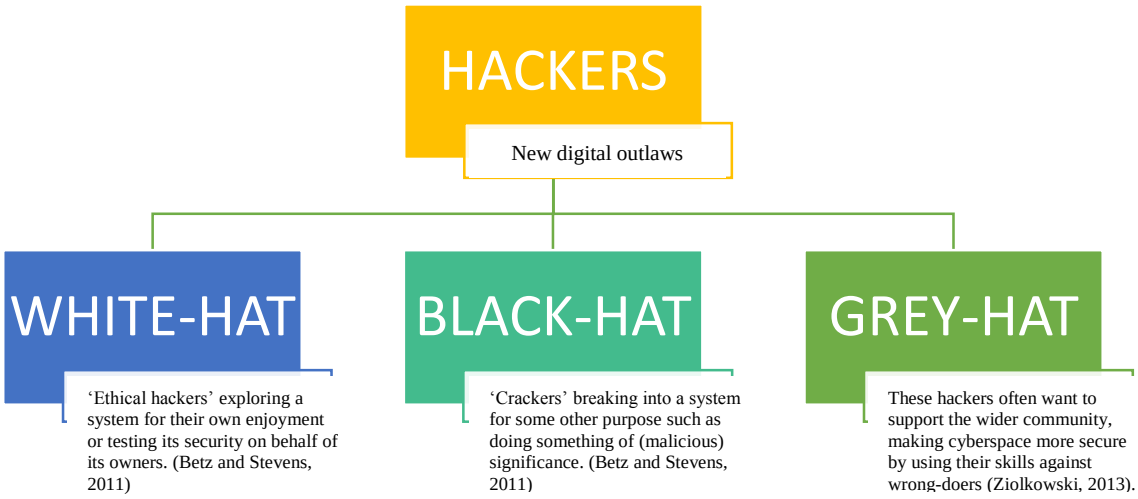
Hackers

In his 2011 article 'A brief history of hacking', BBC reporter Mark Ward emphasized that the word 'hacker' in the 21st century has become synonymous with people who lurk in darkened rooms, anonymously terrorizing the internet. Katharina Ziolkowski (2013) describes them as young individuals who are interested in hacking[2] into information technology (IT) services to satisfy their curiosity or thrill challenges.

Cybersecurity expert Professor Dorothy E. Denning (1999) points at a military attack reported during the 1991 Gulf War, when the U.S. is said to have attacked Iraqi military computer systems with a virus installed in a printer assembled in France and shipped to Iraq via Jordan. The virus reportedly disabled the Windows operating system of infected computers and took out their display and printer controllers (Betz and Stevens 2011).

[2] Breaking into computer systems by circumventing security mechanisms (if actually in place) or the use of vulnerabilities in the architecture or in products used in forming this computer system. Depending on the ICT system at hand, the necessary skills for a successful hack can vary over the full spectrum from simple to highly sophisticated.

Figure 1. *Typologies of Hackers*



Organized Cyber Criminals

According to Dreyfus and Assange (1997), cyber criminals are the largest category and are defined as thieves using diverse and sometimes highly innovative techniques to steal (p. 59-62). They usually work as loose networks and their members may be located in close geographic proximity despite their attacks being cross-national. Cybercriminal experts (Kshetri 2013; Jones 2010) claim that cybercrime hot spots with potential links to crime groups are found in Eastern European and the former Soviet countries. Among them, hackers from Russia and Ukraine are considered the most innovative.

According to one of the world's largest cybercrime studies, the 2011 Norton Cybercrime Report, the per annum cost of global cybercrime is $114 billion. Based on the results of the survey, more than two-thirds of online adults (69 percent) have been a

victim of cybercrime in their lifetime ('Norton Study Calculates…' 2011). The economy of the United Kingdom (UK) alone is said to suffer 27 billion GBP in damages and losses annually from cybercrime (Independent Report 2011).

Hacktivists

Denning (2001) defines *hacktivists* as individuals or groups of individuals who conduct cyber-attacks primarily for political reasons rather than monetary ones. They select their targets with high visibility to deliver the intended political message to the appropriate address. It is hard for potential targets to protect themselves against hacktivists due to the unpredictability of their attack strategies. During attacks, hacktivists commonly use the techniques of either launching Distributed Denial of Service (DDoS)[3] attacks to deny internet connected services or defacing[4] websites. According to BBC, The 2011 Verizon Report informs 855 hacktivist activities around the world in which 174 million records were stolen (Wade Baker 2012).

Cyber Warriors

The website *Techopedia* defines *cyber warrior* as a person who engages in cyberwarfare, whether for personal reasons or out of patriotic or religious belief. Cyber warriors, despite having different forms and roles, all deal with information security. Betz and Stevens (2011) say that cyber warriors are state-employed hackers who are acting in the manner of advanced persistent threat (APT) agents or corporate spies but doing so in

[3] Distributed Denial of Service (DDoS) attack is a method commonly applied by the use of botnets to create vast amount of traffic and direct it to a victim ICT system to the end that this system is overwhelmed and does not operate properly, effectively denying access to the service provided by the attacked system.

[4] Web defacement is an act of hacking: a website is accessed and parts of it changed to the extent that, e.g., pictures or messages of offensive or political nature are shown without the consent of the website's owner.

the cause of specific policy objectives. Chuck Hagel, U.S. Secretary of Defense, announced recently that the Pentagon plans to increase the number of its cybersecurity staff by 2016 (Dune Lawrence 2014). Israel, in its aim of becoming a cybersecurity superpower, has launched a program in preparation of the next generation of cyber warriors while they are still in high school (William Booth 2014).

Industry

Nowadays, the Information and Communication Technologies (ICTs) industry play a strategically important role in many aspects of world economy, politics, and social life. In fact, the private sector owns most of the global communications infrastructure, but there are still some countries where national internet service providers are state-owned or state-controlled. The majority of all security products related to this infrastructure are developed, produced, and provided by ICTs industries. The key players in this industry are Microsoft, the world dominant operating system provider for end-user computers; Cisco, the most important supplier of network devices; and Shadow Server,[5] a major volunteer organization that provides malware protection products and others.

1.2.2 State Actors in Cyberspace

According to Betz and Stevens (2011), 'states are obviously important actors and will continue to be so', but there are some other groups of state actors that actively participate in cyberspace activities such as law enforcement agencies, intelligence services, and armed forces (p. 38).

[5] Established in 2004, The Shadow Server Foundation gathers intelligence on the darker side of the internet. They are comprised of volunteer security professionals from around the world. Their mission is to understand and help put a stop to high stakes cybercrime in the information age.

Law Enforcement Agencies

One of the primary goals of any state is to ensure internal security by enforcing the rule of law. Accordingly, for the states with high internet penetration, this includes the enforcement of law in cyberspace as well. To intercept communication, many states use either special software or the regulatory power over industry operating in their national markets and get unencrypted to encrypted data.[6] Developing such special software requires knowledge and skills not commonly present in law enforcement agencies. As a result, some companies turned to providers of law enforcement agencies with solutions to aid their investigations (Voß 2011).

Intelligence Services

Espionage, despite being a criminal act in national legal systems, is an internationally accepted state practice. Intelligence agencies around the world are racing to acquire more information and expand monitoring capabilities in an effort to advance national security (Lewis 2010; Pelican 2012; Reuters 2012). In fact, very limited information is available about the concrete capabilities of intelligence agencies to the public (Poitras and Gellman 2013; Winter 2013). But the recent scandal initiated by former NSA agent, Edward Snowden, illustrates how states with a decent budget and

[6] See the example of Saudi Arabia and India vs. Blackberry, a company which entered the market with a promise to its customers that all communication and messaging would be protected from eavesdropping by everyone, including States. These States denied Blackberry's new service access to their national markets.

enough soft power can attain access to all sort of data stored in or out of US territory and decrypt most of this data if necessary (Ziolkowski 2013).[7]

Armed Forces

With a rapid evolution in technology, today's armed forces are faced with another set of challenges to keep the fifth domain secure from cyber-attacks. Accordingly, states are under pressure to advance their military capabilities to operate in cyberspace. Jellenc (2012) points to scholars' works (Filiol and Erra) where they have compared current state behavior in and about cyberspace with previous cases of arms races and noticed a new arms race is starting.

According to the results of the 2013 United Nations Institute for Disarmament Research (UNIDIR), over 30 states in 2011 have included cyber warfare in their military planning and organizations. Among them, the U.S., China, and Russia are well-known with their developed cyber warfare capabilities.

1.3 Cyberspace Challenges, Risks and Threats

As noted earlier, there is a growing number of state and non-state actors in cyberspace, who are stealing, changing, or destroying information to cause some disruptions in the internationally interconnected infrastructure. The borderless and anonymous features of the internet blurs the distinction between traditional threat actors. Cyber security experts say that the

[7] According to the documents and information leaked by Snowden, the NSA '[…] have focused on compromising encryption found in Secure Sockets Layer (SSL), virtual private networks (VPNs) and 4G smartphones and tablets. The NSA spent $255 million this year (2013) on the decryption program […] which aims to "covertly influence" software designs and "insert vulnerabilities into commercial encryption systems". In the course of developing the global surveillance system *Prism*, major US companies, and some of the most important global companies to provide widely used services and products, such as Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube and Apple, have been forced to allow NSA direct access to their data. (PoitrasandGellman 2013)

forms of potential threats to information system can be various but indicate ‘attack modes’ as denial, deception, destruction, and exploitation. Such threats can come from a variety of sources such as a foreign government, criminals, terrorists, rival businesses, or simply individual pranksters and vandals (Berkowitz 2003).

Attacks against the information infrastructure have occurred frequently in previous years and, at the same time, perpetrators are becoming more professional. The openness and scope of cyberspace enable hidden attacks and the misuse of vulnerable systems as tools for cyber-attacks possible. Considering the complexity of malware, the possibilities of responding to and retracing attacks are very limited. Accordingly, criminals, terrorists, and spies use this virtual domain for their activities and do not stop at state borders. It is not except that military operations can also be behind such attacks (CSSG 2011).

As cyberspace is becoming the next so-called battleground for military strategists, the world may indeed be witnessing the rise of a new zone of strategic competition. Moreover, they are turning a new virtual domain to ground zero for the next global arms race. Human dependence on technologies and disruptive innovations make online targets increasingly attractive for cyberspace actors to achieve great impact at lower cost (Hughes 2010).

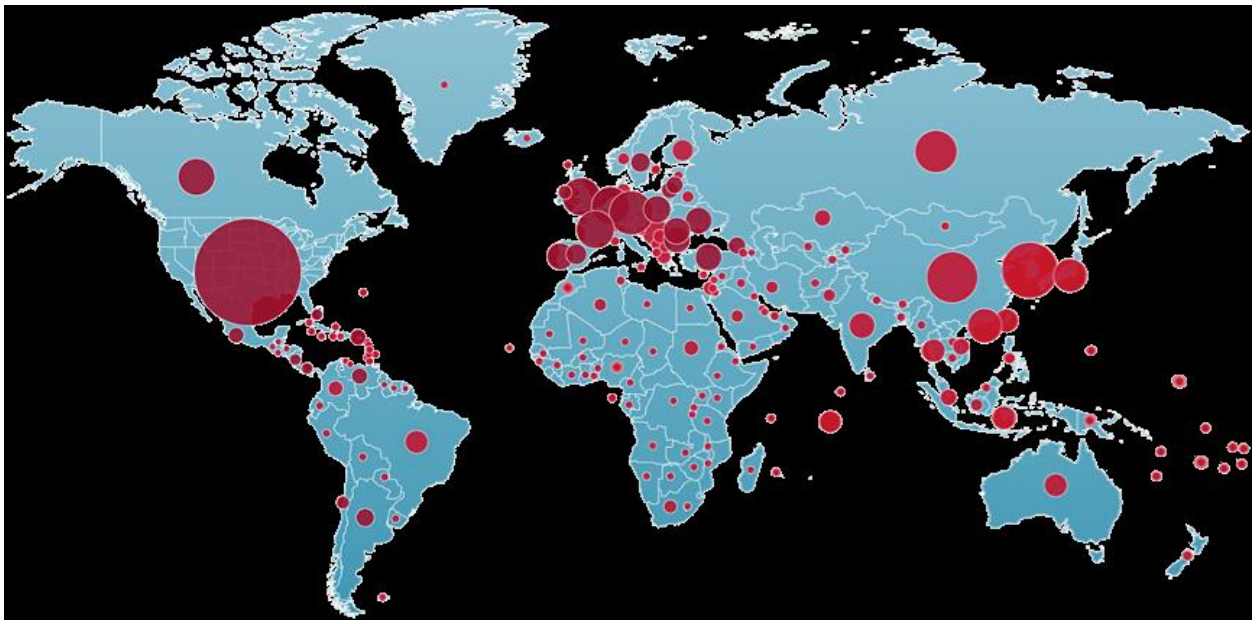
Today, the problem of cyber-espionage is crucial as a number of governments use the internet for cyber-attacks in obtaining secret information. In order to perform cyber-espionage operations, governments increasingly co-operate with private hacker groups that are able to break into corporate databases and steal strategically important knowledge (Bendiek 2012). A substantial increase in both hacking and industrial espionage conducted online presents a significant threat to the national economy (CFECIE 2011). For instance, U.S. officials report that American companies lost $50 billion in 2009 alone due to cyber-espionage (Ryan 2011), and

some analysts report that the worldwide loss due to hacking exceeds $1 trillion (Voigt 2011). As a matter of fact, the greatest possible threat posed by cyber-espionage is simply economic harm. Furthermore, another threat that carries the same amount of importance is the possibility that a foreign military power or terrorist group might use the vulnerability of an information system to facilitate a conventional attack (Berkowitz 2003).

The White House believes that cyber threats can even jeopardize international peace and security more broadly as traditional forms of conflict are extended into cyberspace. Aside from that, U.S. officials claim that technical challenges can be equally disruptive as one country's method for blocking a website can cascade into a much larger, international disruption of the network (ISC 2011).

A World Map of Malware

The network security company FireEye developed a World Map of Malware based on cyber-attacks discovered in 2013. The map illustrates the global nature of cyber threats. The red circles represent initial command-and-control (C&C) hacker infrastructure i.e. the compromised computers and computer addresses from which attackers launched operations in 2013. But it does not mean that the C&C infrastructure was located in those countries. In fact, advanced attackers mostly route or proxy their traffic through multiple intermediate third-party compromised networks, in order to make attribution more difficult for network defenders.



The FireEye reports that the homes to malicious C&C infrastructure in 2013 were the United States (24.1%), Germany (5.6%), South Korea (5.6%), China (4.2%), the Netherlands (3.7%), the United Kingdom (3.5%), Russia (3.2%), Canada (2.9%), France (2.7%), and Hong Kong (1.9%). According to the World Map of Malware, the largest international networks of malicious servers were located in Europe and Asia (Geers 2014).

CHAPTER 2

POWER POLITICS AND CYBERSPACE

2.1 Power Politics in International Relations

Whenever we talk about the international system, the first concept that comes to our mind is power politics. As a matter of fact, power politics still remains a key concept in the discipline of international relations. The concept has a long history of discussion, and scholars still dispute on the role and nature of power. Kenneth N. Waltz (1986) notes that power is a key concept in realist theories of international politics, while conceding 'its proper definition remains a matter of controversy' (p. 333). And Robert Gilpin describes the concept of power as 'one of the most troublesome in the field of international relations' (1981, p. 13) and suggests that the 'number and variety of definitions should be an embarrassment to political scientists' (1975, p. 24).

Michael Barnett and Raymond Duvall (2005) examine power in its different dimensions in global governance. They claim that scholars tend to underestimate the importance of power in international relations because of a failure to see its multiple forms. Moreover, Barnett and Duvall discuss different forms of power that connect and intersect in global governance in a range of different issue areas.

Alexander Wendt differentiates the power politics between three schools of thought in international relations – neorealist, neoliberals, and constructivists. He argues that power politics follows from ideas held by actors and reproduced through process:

> I argue that self-help and power politics do not follow either logically or causally from anarchy and that if today we find ourselves in a self-help world, this is due to process, not structure. There is no 'logic' of anarchy apart from the practices that create and instantiate one structure of identities and interests rather than another; structure has no existence or causal powers apart from process (Wendt 1992, p. 394)

2.1.1 Power Politics from Neorealist and Neoliberalist Approaches

Despite the fact that Realism provides an unsatisfactory theory of world politics, theorists (Morgenthau 1966; Keohane 1968) state that 'realism is a necessary component in coherent analysis of world politics because its focus on power, interests, and rationality is crucial to any understanding of the subject'. Realists claim that states struggle for power under conditions of anarchy to maximize their security and guarantee their survival. Due to the absence of a higher authority in the international system, states depend upon their own efforts to secure themselves from the predations of other states. Although realism allows for domestic politics, non-state actors, and other forces beyond the state itself to play an important role in determining international behavior, these forces do not challenge the primacy of states and state interests in international politics (Reardon and Choucri 2012).

Joseph S. Nye Jr. (2004) points out that most theorists of international relations suffer from being in the middle of events, rather than viewing them from a distance. He argues that the international relations theory has always been strongly affected by current political concerns. Thucydides, the founding father of realism, presented a structural account of the origins of the Peloponnesian War in part because of the lessons he wished to teach his fellow citizens (Kagan, 1969), and Hans J. Morgenthau (1960) wrote in his post-war classic, *Politics Among Nations*, that he was clearly intent on instructing *his* fellow citizens about the importance of avoiding the idealist and isolationist fantasies of the interwar period (p. 21).

Morgenthau (1946) states that international politics is a struggle for power not only because of the inherent logic of a competitive realm such as world politics, but also because of the 'limitless character of the lust for power [which] reveals a general quality of the human mind' (p. 194). As Waltz (1959) states, Morgenthau is not satisfied to see power as an instrument

for the achievement of other ends in a competitive world, but also thinks that because of the nature of human beings, power is an end in itself. Robert O. Keohane (1986) believes that Morgenthau's definition of power was unclear, since he failed to determine power as a resource (based on tangible as well as intangible assets) and power as the ability to influence others' behavior. For classical realists, Mearsheimer (2001) claims that power is an end in and of itself, however, for neorealists, power is a means to an end and the ultimate end is survival.

For most academics, neorealism can be been seen in Kenneth Waltz's *Theory of International Politics* (1979). His theory highlights the importance of the structure of the international system and its role as the primary determinant of state behavior (cited in Lamy 2001, p. 183). Waltz and other neorealists (Baylis and Smith 2001) see power as the combined capabilities of a state. They claim that states are distinguished in the system according to the power they acquire, not by their function. In fact, power gives a state a place or position in the international system which shapes the state's behavior. For instance, during the Cold War, there were only two states in the international system - the US and the USSR who were positioned as super powers.

Waltz's third major concept 'balance-of-power' simply discusses the outcome of states' behavior predicted from the structure of the international system. A system is a set of interacting units having behavioral regularities and identity over time. The structure of a system determines the ordering of its units. Moreover, it involves an ordering principle, specification of the functions of different parts, and the distribution of capabilities. In international politics, the ordering principle is anarchy, which means the absence of a higher government above states. Realists believe that the specification of differentiation drops out because states perform similar functions in the international system. Thus, the distribution of capabilities (multipolarity,

bipolarity) predicts variations in states' balance-of-power behavior (Nye 2004, p. 25). Furthermore, as Waltz pointed out:

> The problem is not to say how to manage the world, including its great powers, but to say how the possibility that great powers will constructively manage international affairs varies as systems change. (Waltz 1979, p. 210)

Accordingly, Waltz states that a good theory of international politics must be systemic, since the way in which relationships among states are organized strongly affects how government behave toward one another. A system, for Waltz, consists of a set of interacting units exhibiting behavioral regularities and having an identity over time (Keohane 1986, p. 15). Keohane argues (cited in Nye, 2004) that Waltz's spare structural definition of system ignores international economic processes and institutions that can also have strong effects on the way in which states behave. Ruggie also believes that Waltz has been too quick in assuming that the differentiation in units can be dropped as a characteristic of the structure of the international system. He argues that, states may be the dominant units and play a similar functional role in the short term, but whenever other units grow in importance the roles may change (p. 26). Gilpin (1981) differentiates three broad types of changes characteristic of the international system: changes dealing with the nature of the actors or diverse entities that compose an international system known as systems change; changes in the form of control or governance of an international system named simply systemic changes and; the third type of change occurs in the form of regular interactions among the units in the international system labeled as interaction change (p. 39-40). Gilpin (1981) further notes that the latter change is understudied but that it is 'particularly relevant in the present era, in which new types of transnational and international actors are regarded as taking roles that supplant the traditional dominant role of the nation-state, and the nation-state itself is held to be an increasingly anachronistic institution' (p. 41).

Joseph Nye (2004) states that realist theory is better at explaining interactions while liberalism better explains the theory of interest. Liberal theory provides a useful supplement to realism by pointing out how domestic and international factors interact to change states' definitions of their interests (p. 24). The liberal tradition of international relations considers both domestic political institutions and culture as well as international affairs of non-state actors and social processes. Liberal theorists believe that preferences and behaviors of a state is shaped by both domestic and international civil society (Reardon and Choucri 2012).

David Baldwin (1993) identified four varieties of liberalism that influence contemporary international relations: commercial liberalism refers to theories linking free trade and peace; republican refers to theories linking democracy with peace; sociological liberalism refers to theories linking transnational interactions with international integration; and liberal institutionalism refers to the theories of international regimes. In the academic world, the neo-liberal approach refers to neo-liberal institutionalism known as the institutional theory (Lamy 2001). For neo-liberal institutionalists, 'institutions' play a role of the mediator and the means to achieve cooperation among actors in the system. Neoliberals do understand that it may be hard to achieve cooperation in the absence of mutual interest. However, they believe that states cooperate to achieve absolute gains and 'cheating' or non-compliance by other states is the greatest obstacle for cooperation (Lamy 2001, p. 189-191).

Neoliberals and neorealists both agree that both national security and economic welfare are important, but they differ in relative emphasis on these goals. Powell (1991) constructs a model intended to bridge the gap between neoliberal emphasis on economic welfare and neorealist emphasis of security. In his model, states are assumed to be trying to maximize their economic welfare in a world where military force is a possibility (Baldwin 1993, p. 7). Joseph

M. Grieco (1988) argues that neoliberals and neorealists basically have different visions on the nature and consequences of anarchy. He affirms that the neoliberal institutionalists do not consider worrying about survival as an important motivation for state behavior as he thinks it is a necessary consequence of anarchy.

2.1.2 Power Politics from a Constructivist Perspective (A. Wendt's theory of anarchy)

Neorealism and Neoliberalism both claim that the world system is anarchic meaning that there is no universal government. According to Keohane (1986) and Mearsheimer (2001), states exist in a self-help world where gains (relative: Keohane, Grieco; or absolute: Waltz, Mearsheimer) matter. Constructivists argue that many of the structures practices of international politics are based on socially-constructed identities, worldviews, and ideas, rather than material forces. Due to this, these structures and patterns of interaction can be shaped according to changes in the ideas and assumptions of the actors regarding the nature of the world. Consequently, the exchange of ideas through 'communicative action' can have an important effect on international relations that is independent of any change in underlying material conditions (Reardon and Choucri 2012, p. 5).

Wendt (1992) has made a sizeable contribution to the social constructivism with his article "Anarchy is what States Make of it: The Social Construction of Power Politics." In this work, he explicitly sums up the central claim of social constructivism. He sees the debate between neorealism and neoliberalism as being more concerned with the issue of whether state action is influenced more by structure (anarchy and the distribution of power) or by the process (interaction and learning) and institutions. Both theories of neorealism and neoliberalism share

generally similar assumptions about agents in that states are the dominant actors in the system. For both theories, the actors define security in terms of 'self-interest' (p. 391-2).

There are social theories that seek to explain identities and interests but do not take interests and identities as given. According to Wendt (1992), they all focus on an inter-subjective conception of a process in which identities and interests are derived from interaction, rather than being formed prior to interaction. Whereas the neorealists treat the self-help and competitive power politics as simply given by the structure of the state system, Wendt argues that collective meanings constitute the structures which organize our actions, and actors acquire identities by participating in such collective meanings. Identities are the basis of interests, and actors define their interests in the process of defining situations. Institutions are relatively stable sets of identities and interests. Self-help is one of such institutions, which combine various structures of identities and interests that may exist in the condition of anarchy (p. 393-9).

Wendt thinks that we assume too much if we conceive of states in the state of nature before their first encounter with each other. We would then also assume too much if we argue that, in the condition of anarchy, states in their natural state necessarily face a 'stag hunt' or 'security dilemma' (Waltz 1946; Jervis 1978). Such claims presuppose that actors have acquired selfish identities and interests prior to their interactions. Instead, self-help emerges only out of interaction between states. If states find themselves in a self-help system, this is because their practices made it that way. Changing the practices will change the intersubjective knowledge that constitutes the system. This does not mean, however, that self-help system, like any other social system, can be easily changed, since once constituted it becomes part of the self-identity of actors. Intersubjective understandings and expectations may have a self-perpetuating quality

constituting path-dependencies that new ideas about self and other must transcend (Wendt 1992, p. 400-11).

The fact that through practice agents are continuously producing and reproducing identities and interests, but does not mean the choices may be experienced with meaningful degrees of freedom. Wendt gives three institutional transformations of identity and security interest, which are by practices of sovereignty, by an evolution of cooperation, and by critical strategic practice (Wendt 1992, p. 412-22).

2.2 Power in Cyberspace

The rules, structures, and institutions that guide, regulate, and control social life are fundamental elements of power. In order to understand how global activities are guided and how world orders are produced, it requires careful and explicit analysis of the working of power (Barnett and Duvall 2005). Betz and Stevens (2011) point out that power does not exist without the relationships through which it is manifest. The operations of power may release the potency of an actor's capabilities, however without these social interactions, these capabilities may as well not exist. Power is not given naturally instead somehow must be produced. Thus, it is only achievable by the effects it has on others. Power, therefore, can be characterized as 'the production, in and through social relations, of effects on actors that shape their capacity to control their fate' (Barnett and Duvall 2005, p. 3). Harold Lasswell and Abraham Kaplan (1950) make a distinction between the old 'power-of-resources' approach and new 'relational power' approach, which developed the idea of power as a type of causation. In other words, power is as a relationship in which the behavior of actor A at least partially causes a change in the behavior of actor B. 'Behavior' in this context includes beliefs, attitudes, preferences, opinions,

expectations, and emotions. In this view, Baldwin (2012) argues, power is an actual or potential relationship between two or more actors (persons, states, groups, etc.), rather than a property of anyone of them (p. 274).

Within politics and strategy, the predominant conception of power is one of direct coercion. This view is intellectually indebted to Max Weber (1948), who defined power as 'the chance of a man or of a number of men to realize their own will in a communal action even against the resistance of others who are participating in the action' (p. 180). The most relevant and common place definition of this form of power is that in which 'the central intuitively understood meaning of [power is where] ... *A* has power over *B* to the extent that he can get *B* to do something that *B* would not otherwise do' (Dahl 1975, p. 201-15). If we apply this idea of power to states, then it is the ability of one state to mobilize its resources in order to advance its interests against the interests of another (Betz and Stevens 2011). In the 1970s, the sociologist Steven Lukes pointed out that ideas and beliefs also help shape others' preferences, and one can also exercise power by determining the wants of others. Later, Nye (2004b) distinguished between hard and soft power along a spectrum from command to cooptive behavior. Hard power behavior rests on coercion and payment. Soft power behavior rests on framing agendas, attraction or persuasion.

Indeed, it is hard to define the concept of power, therefore power in cyberspace assumes the same difficulty as well. However, power in cyberspace can be described by the dimensions of power in creating social order and domination. Here, we again enter into the realm of individuals and collectives in cyberspace. Although, such argument does not put cyberpower in the context of power per se but the power that resides in cyberspace (Arumpac 2006). Daniel T. Kuehl (2009) defines cyberpower as the ability to use cyberspace to create advantages and influence

events in all other operational environments and across the instruments of power. Since cyberspace is simply an environment, cyberpower is a measure of the ability to employ that environment. Technology is one of obvious factors of the elements of power, which acquires the ability to enter to cyberspace and makes it possible to use it. Another important factor is organizations that we create. Organizations reflect human purposes and objectives, meaning that their perspectives on the production and exercising of cyberpower will be shaped by their organizational mission, be it military, economic, or political. All of these different factors shape how we employ cyberpower to impact and influence the elements of power (Kramer et al. 2009).

Strategists Betz and Stevens (2011) claim that, 'what we decide to include or exclude from cyberspace has significant implications for the operations of power, as it determines the purview of cyberspace strategies and the operations of cyber-power' (p. 36). Scholars have determined four basic forms of power that operate in cyberspace: compulsory, institutional, structural, and productive. Compulsory cyber-power takes place when one cyberspace actor uses a direct coercion against another one in order to change his behavior and conditions of existence. This form of cyber-power can be found in the interactions between non-state actors and states as well as between non-state actors. Institutional cyber-power exists when one cyberspace actor controls another one through the mediation of formal and informal institutions. Structural cyber-power is the form of power that operates to maintain the structure in which all actors resided and regulate the actions that actors may wish to take with respect to others. Productive cyber-power defines the 'field of possibility' that compel and facilitate social actions (Barnett and Duvall 2005). In fact, the forms of cyber power described above do not exist separate from one another. Accordingly, if one wishes to define the operation of power in cyberspace then he needs to take

into consideration the actual or possible presence of all powers. The conception of cyber power may be incomplete if any form is not considered (Betz and Stevens 2011).

In fact, cyber-power affects many other domains from politics to economics. It can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace. Accordingly, Nye (2010) states that we can distinguish 'intra cyberspace power' and 'extra cyberspace power' just as with sea power, we can distinguish naval power on the oceans from naval power projection onto land.

Table 1: Physical and Virtual Dimensions of Cyberpower

	Targets of Cyberpower	
	Intra cyberspace	**Extra cyberspace**
Information Instruments	Hard: Denial of service attacks Soft: Set norms and standards	Hard: Attack SCADA systems Soft: Public diplomacy campaign to sway opinion
Physical Instruments	Hard: Government controls over companies Soft: Infrastructure to help human rights activists	Hard: Bomb routers or cut cables Soft: Protests to name and shame cyber providers

Table 1 shows how physical instruments can provide both hard and soft power resources that can be used inside and outside cyberspace.

Source: Joseph Nye Jr. 2010, p.5

Cyber information that travels within cyberspace may create soft power by attracting citizens in another country. For example, a public diplomacy campaign over the internet may be considered soft power. If that cyber information presents some damage to physical targets in

another country, then it becomes hard power. Many modern industries today are controlled by computers linked in Supervisory Control and Data Acquisition (SCADA) systems. Thus, if any malware intervenes in these systems, then it can cause real physical effects.

Physical instruments can allow power resources to affect the cyber world. For instance, the means of technology such as physical routers, servers, and fiber optic cables that carry the electrons of the internet have geographical locations within governmental jurisdictions, and companies running and using the internet are subject to the laws of those governments.

Cyberpower creates a balance between other elements and instruments of power and connects them in order to improve all of them. For example, in the past only governments could speak to another governments. But, today, governments and individuals can interact with each other even across national borders. Cyberspace and cyber power present countless ways to drive and facilitate changes (Kuehl 2009).

2.2.1 Security dilemma in a virtual domain

Cyberspace, unlike air, space, or sea, is an entirely man-made realm, at all times shaped by economic and political forces (Deibert et al. 2008). The geography of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a switch. (Rattray 2009, p. 256) Security in this virtual environment is closely connected to the new vulnerabilities originated from the application of the information and communication technologies to all political and societal projects (Cavelty et al. 2007). The source of these vulnerabilities may be a number of empowered cyberspace actors such as individuals, private, corporate, commercial, and political, governmental and intergovernmental, inter- and transnational entities. Due to increasing cyber-threat, it has become as a strategic military concern and today, meaning that many governments

have or want to acquire offensive cyber ‘weapons’. For instance, Iranian and Indian governments turn a blind eye to hackers who work in the interest of the state. The White House’s 2011 International Strategy for Cyberspace states that the U.S. reserves the right to retaliate against hostile acts in cyberspace with military force. Due to anonymity of cyberspace, uncertainty and mistrust are increasing which, in turn, demonstrates the first sign of a ‘cyber security dilemma’. (Cavelty 2012). A ‘cybersecurity dilemma’ exists when efforts by one state to enhance the security of its digital infrastructure, either through the development of offensive or defensive cyberwarfare capabilities, decrease the cybersecurity of others. Deibert and Crete-Nishihata (2012) also point out the character of global relations may be shaped by negative international dynamics. For instance, states compete against each other in cyberspace. They make an effort to advance their national armed forces capabilities to fight and win wars in this virtually strategic domain. Their competitive and threatening approach to cyberspace can impact the decisions they make. When one government sees another doing something, the pressures may build to act likewise or risk being left behind (Goldstein 2003, p. 237-67).

Because of the presence of high risk and urgency, the extreme form of imitation and learning occur around national security issues (Deibert and Crete-Nishihata 2012). For instance, after the Hacking Back report was released, former U.S. Director of National Intelligence Dennis Blair asserted that U.S. policy makers should consider more aggressive solutions against the increasing threat of cyber-espionage (Smith 2010). Afterwards, as the Indian government was worried about spying and sabotage from its neighboring countries, particularly China and Pakistan, it began readying a cyber-army to hack into hostile nation’s computer systems (Singh 2010).

Consequently, as it is known in the international system, we are now entering into a classic 'security dilemma' in which dozens of governments imitate the actions of states and perceived intentions in order to legitimate the necessity and development of offensive cyberwarfare capabilities. According to arguments of international relations theorists, cyberspace has many characteristics related to the logic of the security dilemma: offense is considered to be overwhelmingly dominant (Herz 1950; Butterfield 1951); deterrence is difficult to implement due to problems around attributing the source of cyber-attacks; there is a lack of transparency around many cyberspace information operations, which are typically undertaken behind a veil of secrecy; and, finally, the barriers to entry are low, to the point where even individuals can participate in consequential cyber-attacks (Deibert et al. 2008). Thus, Nicholas C. Rueter (2011) claims that due to the unique properties of cyberwarfare, the cybersecurity dilemma may be more difficult to break than the typical security dilemma. Myriam Dunn Cavelty (2014) stresses that a solution to this dilemma is achievable if a cyber-security policy is based on strong consideration for privacy and data protection and also emphatically against vulnerability. Some state actors, who want national security that extends to cyberspace, can consider such solution as a compromise. If they do not, then the quest for more national security will always mean less cyber-security, which will in turn always mean less national security due to vulnerabilities in critical infrastructures.

CHAPTER 3

INTERNATIONAL NORMS IN CYBERSPACE

3.1 NATION-STATES IN CYBERSPACE

Barlow stated the following,

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us (Barlow 1996, p.1).

Barlow claimed to be building a new community in cyberspace with its own norms and internal regulator practices where governments were neither invited nor deemed necessary (cited in Betz and Stevens 2011, p. 56). The question then becomes what is to be done with the increasing number of incidents and the awareness of cybercrime. As a matter of fact, adequate security will not be provided in the absence of government intervention.

Senior government leaders and industry executives are deeply concerned regarding the growth of cybercrime, cyber-espionage, and even cyber wars, threatening a globally-networked society. For instance, in 2007, Russian Business Network (RBN) accounted for approximately 40% of the global cybercrime turnover, considered to cost more than 100 billion USD (Klimburg 2011). The Information Warfare Monitor Project,[8] established in 2002 by a group of cyber-security experts (R. Deibert, R. Rohozinski, J. Palfrey, J. Zittrain), after a deep investigation has discovered a cyber-espionage network named GhostNet that is based mainly in China. A complex system of cyber-espionage systematically targeted and compromised computer systems of the Tibetan government, India, the United Nations, and several other countries.

A world where cyber-espionage and cybercrime are largely risk-free requires explicit norms for state behavior reinforced with explicit understandings on outcomes and responses. In

[8] The Information Warfare Monitor project closed in 2012.

fact, norms are a driving factor as they shape international opinion and affect political decision by national leaders. Since norms need not take the form of binding agreements, it is easier to obtain multilateral agreements to these norms. It is obvious that in a high level risky environment where no one trusts each other, agreements reducing risk may be achieved gradually, after a sequence of first confidence-building measures to create the trust necessary for agreement, then norms for state behavior, and finally, perhaps, some binding agreement (Lewis 2013, p. 53).

As soon as the UN resolution on supporting discussions of cyber norms was accepted, several countries and groups of countries have presented broad strategies on state behavior in cyberspace for conducting more secure and stable international activities in this virtual domain. The existence of shared understandings about the acceptable behavior of nation-states in other domains of global commons stabilizes and provides a basis for international action when appropriate measures are required. Respecting such norms helps to prevent misunderstandings that could lead to conflicts. The International Strategy (2011) points out that the creation of international norms for state behavior in cyberspace does not require a reinvention of traditional international law. Established international norms navigating state behavior in other domains can also apply in cyberspace. However, the ubiquitous feature of this virtual realm requires additional work to define how these norms apply and what other supplementary understandings to be required.

Since nation-states do not recognize the importance of existing international legal norms, they forget to consider two main issues – respect for sovereignty and non-intervention in the domestic affairs of other states. But propagating internet freedom globally by supporting 'civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association' creates political concern for governments that do not respect free speech and

democratic politics (White House 2011, p. 23). Some nation-states perceive cyberspace as a source of threats to their domestic sovereignty. As a matter of fact, there is no clear example of this dynamic, but there are a number of states who currently endeavor to control their citizens' access to information on the basis that certain types of 'content' and activities constitute threats to internal order and authority, as well as to established economic practices. (Betz and Stevens 2011, p. 65)

In fact, cyberspace is continuously being shaped by policies adopted by states to utilize the extra-territorial realm of the internet to the best of their ability. Indeed, there is every reason to assert that states are collectively enforcing their authority in cyberspace. Consequently, we have not witnessed the end of the nation-state, but a return to overlapping authorities, including various forms of governance structures (Cavelty 2007, p. 152). The OPI discovered that the growing use of internet 'filtering' techniques are found particularly in the Middle East, Asia, and former Soviet countries, but also in Europe, Australia, and North America (Deibert et al. 2008).

Any malicious behavior in cyberspace creates a state of urgency and alarm for governments, diplomats, and private sector companies. They start to consider whether current norms need modification or if new 'cybersecurity norms' are necessary. The question then becomes what happens when those international norms are infringed upon by governments themselves. This chapter provides arguments of some scholars on how and why nation-states infringed upon international norms of state behavior in cyberspace through network stability and reliable access.

Deibert (2003) highlights the fact that the creators of the internet consciously designed it to be open and built into its architecture. So its openness could enable political actors contend the shape of this architecture. Such dichotomy impacts the relationship between technologies and politics, and clarify the mutually-embedded relationship between the two. Gerald Stang (2013)

emphasizes that cyber conflict involving states will diminish and move along with the quality of the relationship between those states, but states engaged in contest will continue testing each other's cyber capabilities.

3.1.1 Network Stability

> ***States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure.***
>
> International Strategy for Cyberspace 2011

Nation-states maintain an important role by guaranteeing national security and protecting private property, however their possibilities to act in the borderless domain are extremely limited. Thus, it is highly important that different national regulations are concerted at the international level. In many countries, breaking into foreign databases, for instance, constitutes no offense as long as direct damage is not detectable and accordingly, the way in which governments would react remain unclear. There are number of important formal and informal governmental and non-governmental actors that deal with cybersecurity issues and operate at the international level. The General Assembly of the United Nations play a central role in the issue of cybersecurity issue as well as organizations such as the International Telecommunication Union (ITU), the Group of 20 (G20), the Group 8 (G8), NATO, the Shanghai group, and Interpol also play a significant role.

The world is organized around nation-states and national governments, and every physical artifact of information technology is located somewhere. Consequently, one might expect

cyberspace-related tensions to arise between nations exercising sovereignty over their national affairs and interacting with other nations (Charney et al. 2009, p. 6). Proponents of cyberspace sovereignty usually present a normative argument, which is that nations should respect the rules of cyberspace. There are many scenarios in which nation-states arbitrarily intervene into the internationally interconnected infrastructure to exercise their power or demonstrate their cyber capabilities.

RUSSIA

As many cyber security researchers agree today, Russia has the world's best hackers and high-technology capabilities that enable them to do various cyber operations without being caught. In fact, Russia has been accused of being behind several of the best-known politically motivated cases of international cyber conflict to date. Russia was suspected in 2007 in using cyber-attacks in retaliation against Estonia, one of the most wired countries in Europe, for having moved a Soviet-era statue (Joshua Davis 2007). In 2008, Russia was again the prime suspect in denial-of-service (DoS) attacks on Georgian government websites. U.S. Deputy Secretary of Defense William Lynn said that these cyber-attacks, USB-vector attacks on Central Command (CENTCOM), were the "most significant breach of U.S. military computers ever" (Lynn J.W. 2010). In 2009, Russian security services were blamed in another leak scandal known as 'Climategate'. Russian hackers were suspected, because the explosive hacked emails from the University of East Anglia were leaked via a small web server located in Siberia. The purpose of this cyber-attack was to undermine the Copenhagen summit on global warming (Will Stewart 2009). In 2010, Alexey Karetnikov, a Microsoft software tester was suspected of spying and further deported to Russia (Anastasia Ustinova 2010). In 2014, a cyber-security company named

FireEye reported about more sophisticated cyber-attacks backed by the Russian government against NATO, the EU, and government ministries.

Today, Russia plans to create special cyber defense units to protect the country against online warfare. The formation of units will be conducted in stages and will be completed by 2017 (Vadim Gorshenin 2013; Geoffrey Ingersoll 2013; Military and Intelligence 2014).

CHINA

Based on the string of cyber operations implemented by Chinese hackers against other governments and organizations, cyber defense experts argue that the most energetic cyber warriors are Chinese. In 1999, top officials in the Clinton administration warned that China posed an "acute intelligence threat" to the government's nuclear weapons laboratories (Gerth 1999). In 2001, Chinese hackers threatened the U.S. government that it would launch an attack to government and company websites in retaliation for the mid-air collision between a Chinese fighter jet J-8II and a U.S. Navy EP-3 signals intelligence (SIGINT) aircraft (Wagstaffi 2001). In 2009, Citizen Lab researchers discovered the existence of GhostNet - a malware-based cyber-espionage network of over 1,295 infected computers in 103 countries, 30% of which were high-value targets such as ministers of foreign affairs, embassies, international organizations, news media, and NGOs (Information Warfare Monitor 2009). Aside from that, the Pentagon reported in 2009 that computer spies had breached the most advanced U.S. fighter jet project and blamed on it the Chinese military (Siobhan Gorman 2009). Recently, Chinese hackers have attacked America's defense establishment, as well as Google, Intel, Adobe, RSA, Lockheed Martin, and Northrop Grumman, the New York Times, the Wall Street Journal, and the Washington Post (Gross 2011; Perlrot 2013). In 2013, U.S. cyber security experts strongly suspected China's

military in a cyber-attack against 23 natural gas pipeline operators to steal crucial information that could compromise security (Clayton 2013). In the same year, Chinese hackers were again suspected by US intelligence agencies for the cyber intrusion into sensitive U.S. Army Corps of Engineer's National Inventory of Damns (Gertz 2013)

In turn, Chinese officials also claim that their country is not excluded in being a target of cyber-attacks operated by other governments. In 2006, the China Aerospace Science and Industry Corporation (CASIC) found spyware on its classified network. In 2007, the Chinese Ministry of State Security said that foreign hackers, 42% of which were Taiwan and 25% of which were American had been stealing information from Chinese key areas. In 2009, Chinese Prime Minister Wen Jiabao announced that a hacker from Taiwan accessed a Chinese State Council computer in order to steal the draft of the National People's Congress Report (CSIS 2006). In 2013, Edward Snowden, the NSA whistleblower, told China Press that the U.S. government spied on universities in China and further collected information from mobile phones. Thus, this means that U.S. spy agencies had been watching China and Hong Kong for years (Rapoza 2013). In the same year, China claimed that the Chinese computer emergency response team (CERT) reported "mountains of data" cyber-attacks by the U.S. (Hille 2013).

THE UNITED STATES

Cyber security expert Ralph Langner (2011) states that the U.S. is the only cyber superpower in the world and that Stuxnet[9] is the only true cyber-attack the world has ever seen. According to a New York Times report, the attack could have been authorized by the Bush administration and sped up by the Obama administration (Lemos, 2011). David E. Sanger (cited in Geers 2014) argues that the most amazing thing about Stuxnet was its true purpose was

[9] A worm created jointly by the US and Israel in order to attack Iran's nuclear programme.

changing the course of world history. It was designed to help prevent an expansion of the world's most exclusive club, the "nuclear club." To some degree, that means that Stuxnet replaced a squadron of aircraft that would have violated foreign airspace and left a smoking crater in the Earth's surface. Richard Clarke, America's longtime counterterrorism czar, disclosed that the U.S. government is engaged in a very different, very dramatic and new way of using its cyber offensive capability, when he commented on if his government was behind the Stuxnet attack (Rosenbaum 2012). In 2012, Iran was targeted by another espionage malware known as Flame. According to the world's best cryptography experts, this malware could only been developed by world-class cryptographers with the backing of a wealthy nation-state (Goodin 2012). After Stuxnet, the cyberworld has been attacked by some other advanced malware such as Duqu, Flame, and Gauss, which may all have been developed by the same organization or nation (Bencsáth 2012). The news website The *Intercepts* reported that the highly-complex malware known as Regin was used in systematic spying campaigns against governments, businesses, researchers, and private individuals. The malware appeared to be linked to U.S. and British intelligence (Samson 2014).

In response to the U.S. attacks, a group supported by Iran and calling itself the Cutting Sword of Justice hacked the world's most valuable company Saudi Aramco. The virus 'Shamoon' erased data on three-quarters of Aramco's corporate computers replacing all of it with an image of a burning American flag (Perlroth 2012). Another group of hackers, known as Martyr Izz a d-Din al-Qassam Cyber Fighters struck with DDoS attacks against US financial institutions (Walker 2013). In 2013, US officials reported that Iranian-backed hackers had increased surveillance missions against the US cooperation (Gorman 2013).

NSA whistleblower Edward Snowden provided writer James Bamford with previously unreported allegations of NSA cyberattack tools, including a piece of software codenamed MonsterMind,[10] that would automate a hostile response when it detected a network intrusion. Moreover, Snowden also reported that a 2012 incident that took Syria's internet offline was due to a failure of the NSA. On November 29, 2012, the analysis firm Renesys reported that out of 92% of the routed networks providing internet connectivity for Syria, 77% of them had gone dark (Ackerman 2014).

3.1.2 Reliable Access

> ***States should not arbitrarily deprive or disrupt individuals' access to the Internet or other networked technologies.***
>
> International Strategy for Cyberspace 2011

John P. Barlow (cited in Betz and Stevens, 2011) compares cyberspace, in its present condition, with the 19th century wild West in the U.S. It is vast, unmapped, culturally and legally ambiguous, verbally terse, hard to get around in, and up for grabs. Large institutions already claim to own the place, but most of the actual natives are solitary and independent, sometimes to the point of sociopathy. It is, of course, a perfect breeding ground for both outlaws and new ideas regarding liberty. In fact, nation-states have differing visions of cyberspace and any issues related to it such as information access, sovereign authority, and sovereign responsibilities. China and Russia, Hurwitz (2011) argues, have a dissident view of internet freedom and are less concerned than the U.S. about industrial espionage. As a matter of fact, issues related to internet

[10] The MonsterMind software is a digital tool that would detect the beginnings of a hostile cyber incursion and automates a hostile response.

freedom or the free flow of information have been very contentious topics with regard to the role of governments on internet control and its future. Since the rights to information, expression and association have built the use and growth of cyberspace, internet freedom is both a human rights and a cyberspace issue.

Today, more states are engaged in internet control and restrictions on social media. More than forty countries now are involved in developing second and third generation filtering techniques. At the international policy level, many of these same states are trying to create a norm of the state as the final arbitrator of the internet within its territory, through the promotion of the ITU as the appropriate agency for internet governance, and with the disparaging of ICANN[11] and the associated multi-stakeholder model (Hurwitz 2011, p. 20). Due to asserting sovereign control over their national cyberspace, countries are deploying technologies which will allow them enforce control and to create multilateral governance structures to legitimize these actions (Glenny 2010). The most frequently conducted form of state control in cyberspace is internet filtering or censorship, which is the prevention of access to information online within territorial boundaries (Villeneuve 2006). Deibert and Crete-Nishihata (2012) point out that nation-states have various motives for internet filtering within their boundaries. Some states justify internet filtering in controlling access to content that violates copyright, concerns the sexual exploitation of children, or promotes hatred and violence. Other countries filter access to content related to minority rights, religious movements, political opposition, and human rights groups. In China, for instance, any regulation related to internet access and agreements between the government and individual ISPs are carried through legislation. Today, only nine ISPs in China have licenses to provide internet access. Accordingly, the government has centralized control over internet users and information flow within the country (Zittrain and Edelman 2003).

[11] The Internet Corporation for Assigned Names and Numbers

Overall, more than sixty laws limit the content available to Chinese web users. Yet, no standards have been set forth in law as to what content is to be filtered nor is there official admission of filtering (ONI 2004, p. 7).

Since 2003, the ONI has been conducting research on national internet filtering. A study reported that annually more than sixty countries are engaged in some type of internet filtering.[12] In the beginning of this study, only a few governments were involved in internet censorship, however ONI reports later indicates that more than forty countries engage in this practice and a growing number of them are democratic, industrialized countries (see Figure 2). Based on this study, Deibert and Crete-Nishihata (2012) claim that the norm of national internet filtering is growing and the rationale for implementing filtering varies widely from country to country.

Figure 2 shows the results of the 2007-2012 ONI Internet Censorship study. In that period of time, over 70 states were tested on various types of internet censorship which were afterwards categorized according to the following themes: social, political, conflict and internet tools.

[12] ONI uses the following technical methodology to verify Internet censorship. Lists of websites and keywords are collected that cover topics that might be targeted for censorship including pornography, gambling, international and independent news media, human rights, and political content. A data collection software client designed to query these predefined lists of URLs is distributed to researchers within countries suspected of engaging in Internet censorship. The list of URLs is accessed simultaneously over http both in the country suspected of Internet filtering and a country with no filtering regime (e.g., Canada). The data gathered from the country with no filtering is used as a control to compare the data from the country suspected of filtering. Where appropriate, the tests are run from different locations to capture the differences in blocking behavior across ISPs.

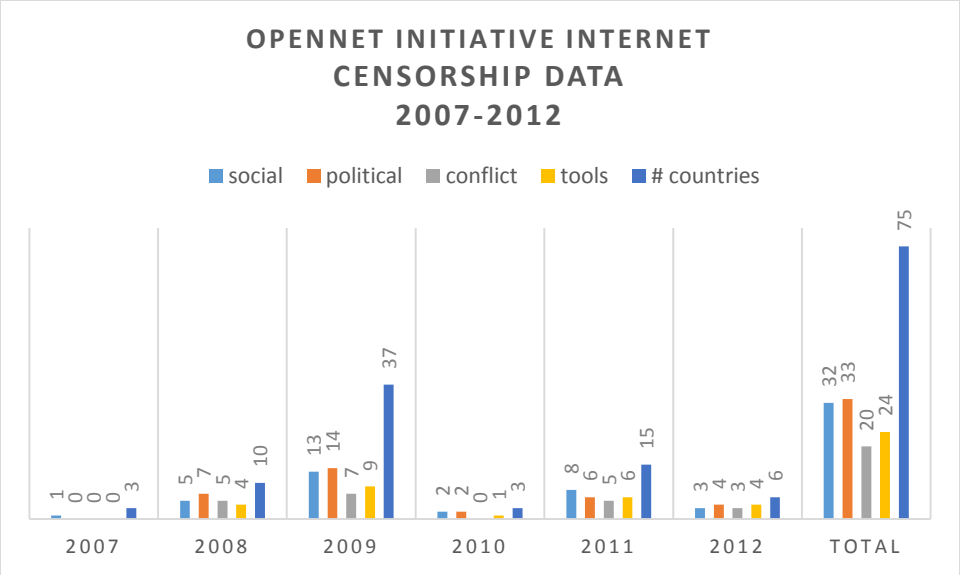


Figure 2

Source: ONI Report 2007-2012

As mentioned earlier, the number of governments employing a broader range of regulatory, legal, covert, and offensive means to cyberspace are increasing which, in turn, explains the fact that the fifth domain is becoming another international strategic zone. The ONI Report indicates the growing number of incidents where governments have blocked access to communication networks for political purposes, especially during elections and public demonstrations. ONI calls these actions 'just-in-time blocking'—a phenomenon in which access to information is denied during important political moments when the content may have the greatest potential impact such as elections, protests, or anniversaries of social unrest. (Deibert and Rohozinski 2008) In 2011, during the Arab Spring, both Egyptian (Dunn 2011) and Libyan (Cowie 2011) governments instituted a widespread shutdown of communication tools. ONI reports from both 2007 and 2009 reveal that shutdown strategy was seen in Nepal (2005), Burma (2007), and China (2009). There are some cases in which democratic states have implemented some form of disruptions of access to communications in response to protests and social unrests.

In 2011, Prime Minister David Cameron delivered a statement to the House of Commons on the disorder and looting that was taking place in London and other cities. He stated that the government is working with the police, intelligence services, and industries to look at whether it would be right to stop people communicating via social media when they know they are plotting violence, disorder, and criminal activities (British PM Speech 2011). Another case related to communication interruption took place in San Francisco in 2011. The Bay Rapid Transit System (BART) shut down its cell phone services to four stations in response to a planned protest in an effort to disrupt its organization (BRTS Report 2011). These examples demonstrate how the government approach to cyberspace has been rapidly changing over the last decade.

The data below provides an overview of the most recent ONI ratings of the breadth and depth of internet censorship in seventy-four countries across four content categories (political, social, internet tools and conflict/security). Thirty-three countries out of 74 have used some type of internet censorship for political purpose. Figure 3 illustrates the relative magnitude of censorship only for a political category:

> **Pervasive filtering (score of 4):** Filtering that is characterized by both its depth—a blocking regime that blocks a large portion of the targeted content in a given category—and its breadth—a blocking regime that includes filtering in several categories in a given theme.
>
> **Substantial filtering (score of 3):** Filtering that has either depth or breadth: either a number of categories are subject to a medium level of filtering or a low level of filtering is carried out across many categories.

Selective filtering (score of 2): Narrowly targeted filtering that blocks a small number of specific sites across a few categories or filtering that targets a single category or issue.

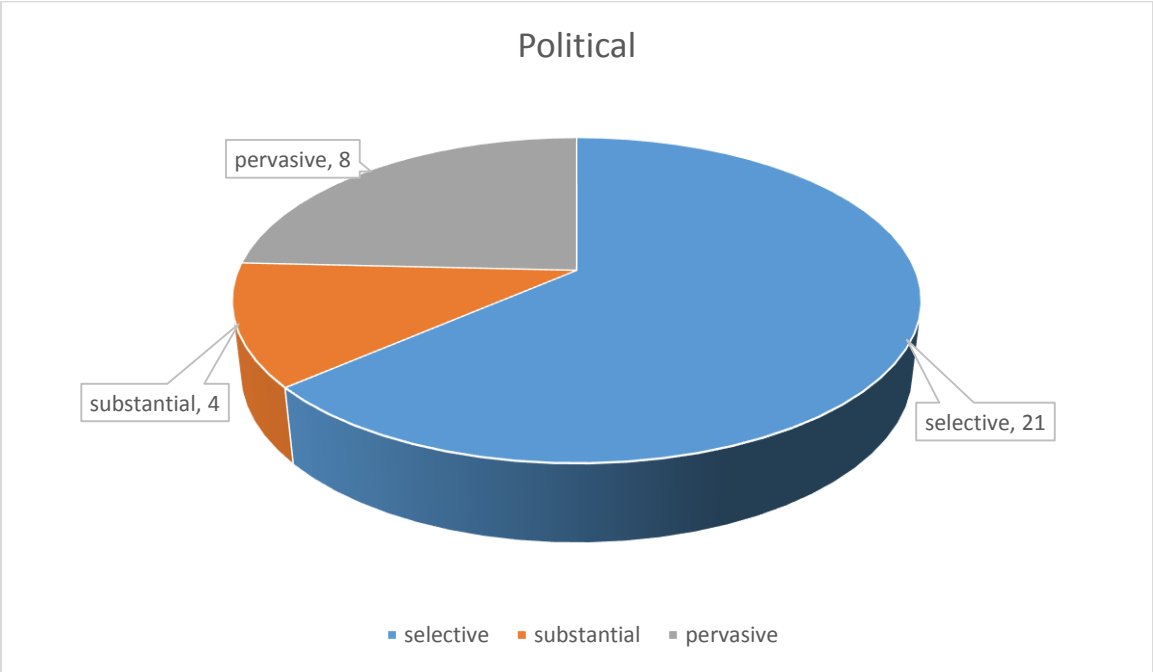


Figure 3 Magnitude of Political Censorship

Source: ONI Reports, 2007-2012

In fact, concerns over the misuse of cyberspace by state and non-state actors for disruptive and malicious activities are growing by day, particularly as cases of cyber-espionage, attacks on critical infrastructure, financial thefts and cyber terrorism are increasing. As soon as cyberspace has become another important arena for human activities, nation-states will not be able to avoid controlling this virtual domain, and, when necessary, will not be able fight for this new artificial environment. The Group of Government Experts (GGE) reports that individuals, groups or organizations, including criminal organizations may act as proxies for states in the

conduct of malicious activities in cyberspace. Moreover, they claim that the absence of a common understanding of acceptable state behavior in cyberspace can endanger international peace and security.

CHAPTER 4

FINDINGS

4.1 Cyber WARFARE[13] vs. COOPERATION

The well-known whistle blower of NSA documents to The *Guardian* and The *Washington Post* said, 'I'm willing to sacrifice all of that because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building' (Meyer 2013).

In 2010, U.S. Deputy Secretary of Defense William J. Lynn declared that the Pentagon had formally recognized cyberspace as a new domain of warfare. Despite the fact that it is a man-made domain, cyberspace has become just as critical to military operations as land, sea, air, and space (Lynn 2010). The growing threat of cyber war requires from governments to develop their cyberspace defense strategies as soon as possible. Many countries, including the United States, are developing weapons for it, like 'logic bombs' that can be hidden in computers to halt them at crucial times or damage circuitry; "botnets" that can disable or spy on Web sites and networks; or microwave radiation devices that can burn out computer circuit miles away (Markoff 2009). For instance, one of the latest the US cyber invention is the MonsterMind software, which is designed to detect the beginning of a hostile cyber-attack and automate a hostile response. With other words, the software can turn a potential act of war into an automated command, without input from the chain of command, and not necessarily target at the perpetrator of the attack, as many such digital penetrations are routed through third countries (Ackerman

[13] Clarke and Knake - "the unauthorized penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the distribution of or damage to a computer, or network device, or the objects a computer system controls."

2014). The most public U.S. cyber-war projects are Plan X, a DARPA (Defense Advanced Research Projects Agency) project for the development cyber warfare technologies that reputable sources claim seeks to track exploitable vulnerabilities of every (civilian, commercial, etc…) device connected to the internet, and ACT (Agile Cyber Technologies), a project developed by Air Force Research Laboratory (AFRL) (Paganini 2012).

Scott Camil, a former sergeant in the U.S. Marine Corps who served four years in Vietnam, says that the number one war crime is starting a war, as all other war crimes emanate from that first crime (cited in Peganini 2012). Accordingly, the decision to develop and maintain the capability for engaging in cyberwar is the first crime, engaging in cyberwar being the second. Cyber security expert, Clarke (2010) states that a cyber-war has already begun as governments are developing strategies and preparing the 'battlefield' to hack into each other's networks and infrastructures. As a matter of fact, the cyber war is 'real' and has a capability to destroy any nation-state.

In a secret U.S. policy document known as Presidential Policy Directive 20, President Barack Obama has outlined details of how the United States conducts offensive operations in cyberspace against other countries (Farnsworth 2013). In 2013, the The *Guardian* published an article that claimed Obama ordered the U.S. to draw up an overseas target list for cyber-attacks. And such an action of the White House may heighten fears over the increasing militarization of the internet (Greenwald 2013). As cyberspace has emerged as a new international battlefield, the armed forces of a number of countries (including China, India, Israel, Great Britain, Iran and Estonia) started to set their cyber units. Moscow takes a guarded view of Washington's activities, believing them to be one of the main causes of the cyber race that has swept the world. In March 2012, Russian officials declared plans to create a cyber-command similar to the one that exists in

the United States. Later on, Vladimir Putin ordered the Federal Security Service (FSB) to develop a national system to forecast and prevent cyber-attacks, giving the agency new powers to fight cybercrime (Chernenko 2013). Specialists say that Russia and China have been supporting an arms control treaty for cyberspace in order to regulate the offensive use of cyber technologies by governments and to block cyber-attacks in the international infrastructure (Markoff 2009). Russia has even drafted a proposal for a Convention on International Information Security (CIIS 2011). But the majority of states, including the U.S. do not see the necessity of such a treaty as they claim that existing rules and law enforcement mechanisms are sufficient (Markoff 2008). As a matter of fact, any agreement on cyberspace presents special difficulties because of issues like internet governance, sovereignty and actors who might not be subject to a treaty. US officials believe that a significant proportion of cyber-attacks against the American government comes from China and Russia. Accordingly, the disagreement over approach impedes cooperation in international law enforcement. Russian officials claim that the absence of a treaty permits a kind of arms race with potentially dangerous consequences (Markoff 2008).

A recent study by the UN Institute for Disarmament Research reports that more than 40 nation-states have now developed some military cyber capabilities, 12 of them for offensive cyberwarfare (UNIDIR 2013). Erika Mann, Executive Vice President of the Computer and Communications Industry Association and a Member of the Board of Directors for ICANN, characterizes the internet as a stimulating and fascinating instrument, 'if you come in with a heavy hand because of threats, you are misjudging the security environment' (Dowdall 2011, p. 5).

The A/65/201 Report points out the increase of ICTs development as instruments of warfare and intelligence, and for political purposes by states. Within the framework of this report, the Group of Governmental Experts offer recommendations for building further cooperation among like-minded partners in order to confront the challenges of the twenty-first century. They believe that the collaboration among States, and between States, the private sector and civil society, is important (Report A/65/201). The UN group of governmental experts do understand the arms control approach can be a starting point of confidence-building measures in cyberspace.

At this point, based on facts mentioned above, I can claim that such behavior of nation-states - disagreements on cybersecurity cooperation and the development of offensive or defensive cyberwarfare capabilities – creates mistrust and competitiveness in the international system which, in turn, decrease the cybersecurity of others. Such consequence of events is familiar to international relations theorists as a 'security dilemma' – 'the tendency for states in a context of uncertainty to defect from cooperative arrangements if they perceive other states' security preparations as threatening (misperception; arms racing)' (Cerny 2000, p. 623). Competitive systems of interaction are prone to security 'dilemmas,' in which the efforts of actors to enhance their security unilaterally threatens the security of the others, perpetuating distrust and alienation. The forms of identity and interest that constitute such dilemmas, however, are themselves ongoing effects of, not exogenous to, the interaction; identities are produced in and through 'situated activity' (Alexander 1981). Wendt (1992) argues that self-help security systems evolve from cycles of interaction in which each party acts in ways that the other feels are threatening to the self, creating expectations that the other is not to be trusted. 'If today we find ourselves in a self-help world, this is due to process, not structure. Structure has no

existence or casual powers apart from process. Self-help and power politics are institutions, not essential features of anarchy. *Anarchy is what states make of it*' (p. 394-95)

In fact, cyberspace is a shared virtual domain which is vast, unmapped and a perfect breeding ground for all actors – state, non-state, criminals, etc - to manifest their power. The internet, is only a set of connections between computers (or a set of protocols allowing computers to exchange information); it can have no impact apart from its use by human beings. (Kalathil 2003, p. 2) Moreover, we should not forget that 'social relations begin and end outside cyberspace'. Thus, based on all arguments provided above, the answer to the question as to why nation-states infringe upon international norms of state behavior in cyberspace is that nation-states with high cyber capabilities are more likely to benefit from anonymity and interconnectivity of this virtual domain to exercise their power internationally by arbitrarily interfering with internationally interconnected infrastructure or using any type of information control techniques. On the contrary, countries with low cyber capabilities prefer to survive in such borderless and competitive domain by denying, disrupting, manipulating their citizens' access to the internet or other networked technologies. In our case, all three nation-states (Russia, China, and the U.S.) have high cyber capabilities, but different political values. Thus, the U.S. with its liberal values supports the free flow of information across borders and wants to maintain its freedom of action in cyberspace. But Russia and China having an authoritarian values (Russia has a semi-authoritarian value) are very concerned on issues related to internet governance, net neutrality, and freedom of speech. Accordingly, Russia and China are actively engaged in various types of internet control activities. This difference on political views and high cyber capability enable these three cyberpowers - Russia, China and U.S. – to manifest their power in this virtual domain by infringing international norms of state behavior in cyberspace. Moreover,

all cases of norm infringement in a virtual domain are directly related to the political conflicts in reality. If this virtual domain became another arena for warfare then this is not because of its ubiquitous or anonymous feature, this is what states make of it.

CONCLUSION

Cyberspace, having a unique feature of transnationality, has formally been recognized as a new domain of warfare just like land, sea, air, and space. As the new domain largely disguises and blurs the identity of cyberspace actors it makes direct attribution impossible. The danger that a humanity faces today comes with the development of digital technologies where aggressive state behavior in cyberspace causes increasing damage and ill-will among nations. Military strategists have been busy adapting their force structures to a new zone of strategic competition for the next global arms race. Russia, China and the U.S. are increasing their budget for cyber-warfare and expanding their offensive capabilities. The military cyber spending of these three countries in 2013 is: United States - $582 billion, China – $132, 203 billion, and Russia Federation – $68, 887 billion (Paganini 2014). States spend hundreds of millions of dollar on building cyber-capabilities in the sense of urgency that other nations have been using cyberspace to attack adversaries or steal secrets. In fact, the U.S. always brands China and Russia as the main source of cyber threats. But with the recent revelation of former NSA agent Edward Snowden on cyberspace offensive operations conducted by the U.S. has encouraged other states to find their own solutions in adapting to a competitive virtual domain.

No doubt that mutual cyber-attacks will continue despite the effort spent by each government to improve the security in cyberspace and prevent infringement within its network.

States do realize that new conflicts will involve new actors in a critical infrastructure such as independent and state sponsored hackers, cyber criminals and cyber terrorists that could create a imbalance among nation-states. Moreover, states do understand that they need to get some norms and rules of state behavior in cyberspace. But due to the different political and social values of each state any attempt to bilateral cooperation turns into a fiasco. For instance, the U.S. with its liberal values is more concerned on industrial espionage, but Russia and China with their authoritarian values have a dissident view of internet freedom. Consequently, there might be little agreement on where to begin and the specification of norms might be slow and piecemeal. As Wendt claimed that international anarchy is a construct, which may be established differently according to perception and attitude of involved states towards each other. So will nation-states change their attitude towards each other on the issues related to security in cyberspace or prefer to keep this 'grey- area' anarchic for arms race and future cyber wars? Moreover, which states will reconsider their political values towards building a cooperation on security related issues in cyberspace?

BIBLIOGRAPHY

Ackerman, S., 2014. *Snowden casts doubt on NSA investigation into security disclosures.* [Online] Available at: http://www.theguardian.com/world/2014/aug/13/snowden-doubt-nsa-investigation-security-disclosures [Accessed 3 December 2014].

Alexander, N., 1981. Situated Activity and Identity Formation. In: *Social Psychology: Sociological Perspectives.* New York: Basic Books, pp. 269-89.

Allison, J., 2002. *Technology, Development, and Democracy.* New York: State University of New York Press.

Anon., 2007. *Nepal.* [Online] Available at: https://opennet.net/research/profiles/nepal [Accessed 3 December 2014].

Anon., 2007. *Pulling the Plug: A Technical Review of the Internet Shutdown in Burma.* [Online] Available at: https://opennet.net/research/bulletins/013 [Accessed 3 December 2014].

Anon., 2010. *US Department of Defense 'Department of Defense Dictionary of Military and Associated Terms'.* Washington DC: US Joint Ghiefs of Staff, Joint Publication 1-02.

Anon., 2011. *2011 report by industry and government on the cost of cybercrime,* s.l.: Cabinet Office and National security and intelligence.

Anon., 2011. *Cabinet Office and National security and Intelligence.* [Online] Available at: https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-government-and-industry-report [Accessed 3 December 2014].

Anon., 2011. *Cyber Security Strategy for Germany,* Berlin: Federal Ministry of Interior.

Anon., 2011. *International Strategy for Cyberspace.* Washington DC: White House.

Anon., 2011. *PM statement on disorder in England.* [Online] Available at: https://www.gov.uk/government/news/pm-statement-on-disorder-in-england [Accessed 3 December 2014].

Anon., 2011. *Report to CFECIE 'Foreign Spies Stealing US Economic Secrets in Cyberspace',* s.l.: Office of the National Counterintelligence Executive.

Anon., 2011. *Russian Foreign Ministry and Security Council 'Convention on International Information Security'.* [Online] Available at: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument [Accessed 3 December 2014].

Anon., 2011. *Statement on temporary wireless service interruption in select BART stations on Aug. 11*. [Online] Available at: http://www.bart.gov/news/articles/2011/news20110812 [Accessed 3 December 2014].

Anon., 2011. *The Cost of Cyber Crime,* Guildford: Detica Limited.

Anon., 2012. *Information Warfare Monitor*. [Online] Available at: http://www.infowar-monitor.net/ [Accessed 3 December 2014].

Anon., 2013. *United Nations Institute for Disarmament Research 'The Cyber Index'*. Geneva: United Nations.

Anon., 2014. *Techopedia*. [Online] Available at: http://www.techopedia.com/definition/28615/cyber-warrior [Accessed 3 December 2014].

Arumpac, A. B., 2006. *A Research Paper on Cyberculture and Virtual Politics.* s.l.:s.n.

Assange, S. D. a. J., 1997. *Underground: Hacking, madness and obsession on the electronic frontier*. Kew: Reed Books.

Babbie, E., 2007. *The Practice of Social Research.* Belmont: Thomson Higher Education.

Baker, W., 2012. *Data theft: Hacktivists 'steal more than criminals'*. [Online] Available at: http://www.bbc.com/news/technology-17428618 [Accessed 3 December 2014].

Baldwin, D. A., 1993. Neoliberalism, Neorealism, and World Politics. In: *Neorealism and Neoliberalism: The Contemporary Debate.* New York: Columbia University Press, p. 377.

Baldwin, D. A., 2012. Power and International Relations. In: *Handbook of International Relations.* s.l.:SAGE, pp. 273-297.

Barlow, J. P., 1990. *Crime and Puzzlement.* [Online] Available at: http://ecstaticsec.tumblr.com/post/94853250039/crime-and-puzzlement-john-perry-barlow-june-8-1990 [Accessed 3 December 2014].

Barlow, J. P., 1996. *A Declaration of the Independence of Cyberspace.* s.l.:s.n.

Barnett, M., 2005. *Power in Global Governance.* First ed. Cambridge: Cambridge University Press.

BART, 2011. *Statement on temporary wireless service interruption in select BART stations on Aug. 11*. [Online] Available at: http://www.bart.gov/news/articles/2011/news20110812 [Accessed 3 December 2014].

Baylis, J., 2001. *The Globalization of World Politics.* New York: Oxford University Press.

Bencsáth, B., 2012. *Duqu, Flame, Gauss: Followers of Stuxnet.* [Online] Available at: http://www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf [Accessed 3 December 2014].

Bendiek, A., 2012. *European Cyber Security Policy.* Berlin: Stiftung Wissenschaft und Politik.

Berkowitz, B., 2003. Cybersecurity: Who's watching the store?. *Issues in Science and Technology,* pp. 55-62.

Betz, D., 2011. *Cyberspace and the State.* London: Adelphi.

Blakely, R., 2010. *India blocks deals with Chinese telecoms companies over cyber-spy fears.* [Online] Available at: http://business.timesonline.co.uk/tol/business/markets/china/article7121521.ece [Accessed 3 December 2014].

Booth, W., 2014. *Young Israeli cyberwarriors learn to duel in the dark.* [Online] Available at: http://www.washingtonpost.com/world/young-israeli-cyberwarriors-learn-to-duel-in-the-dark/2014/10/07/e07a9031-1e01-4815-8938-5fab87495e82_story.html [Accessed 3 December 2014].

Bradbury, D. &. R. R., 2010. *Shadows in the Cloud: Chinese Involvement in Advanced.* s.l.:s.n.

Brenner, S. W., 2014. *Cyberthreats and the Decline of the Nation-State.* s.l.:Routledge.

Broadhurst, R., 2014. Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology,* 8(1), p. 20.

Bumgarner, J., 2009. *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008,* Georgia: US-CCU.

Butterfield, H., 1951. *History and Human Relations.* London: Gollins.

Cavelty, M. D., 2007. *Power and Security in the Information Age.* Hampshire: Ashgate.

Cavelty, M. D., 2012. The Militarisation of Cyberspace: Why Less May Be Better. *NATO CCD COE Publications,* pp. 141-53.

Cavelty, M. D., 2014. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics.*

Charney, S., 2009. *Rethinking the Cyber Threat.* s.l.:Microsoft Corporation.

Chernenko, E., 2013. *Cyberspace looms as new international battlefield.* [Online] Available at:

http://rbth.com/opinion/2013/03/14/cyberspace_looms_as_new_international_battlefield_23875.html [Accessed 3 December 2014].

Clarke, R., 2009. War from Cyberspace. *National Interest 104*, pp. 31-36.

Clarke, R. A., 2010. *Cyberwar: The Next Threat to National Security and What to do About It.* New York: Harper Collins.

Clayton, M., 2013. *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage.* [Online] Available at: http://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage [Accessed 3 December 2014].

Cowie, J., 2011. *Libyan Disconnect.* [Online] Available at: http://research.dyn.com/2011/02/libyan-disconnect-1/ [Accessed 3 December 2014].

Crete-Nishihata, M., 2011. *Egypt's Internet Blackout: Extreme Example of Just-in-time Blocking.* [Online] Available at: https://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking [Accessed 3 December 2014].

Czosseck, C., 2011. Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security. *International Journal of Cyber Warfare and Terrorism (IJCWT),* 1(1), pp. 24-34.

Dahl, R., 1957. The Concept of Power. *Behavioral Science*, 3 July, pp. 201-15.

Davis, J., 2007. *Hackers Take Down the Most Wired Country in Europe.* [Online] Available at: http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all [Accessed 3 December 2014].

Deibert, R., 2008. Access Denied:The Practice and Policy of Global Internet Filtering. In: *Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet.* Cambridge: MIT Press, pp. 123-149.

Deibert, R., 2008. Gyclones in Gyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War. *Security Dialogue 43,* pp. 3-24.

Deibert, R., 2009. Tracking GhostNet: Investigating a Cyber Espionage Network.. *Information Warfare Monitor,* March, p. 53.

Deibert, R., 2011. *Access Contested.* London: The MIT Press.

Deibert, R., 2012. Global Governance and the Spread of Cyberspace Controls. *Global Governance,* pp. 339-361.

Deibert, R., 2012. Gyclones in Gyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War. *Security Dialogue 43,* 1(1), pp. 3-24.

Deibert, R., 2013. *OpenNet Initiative.* [Online] Available at: https://opennet.net/research/data [Accessed 3 December 2014].

Deibert, R. J., 2003. Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millennium - Journal of International Studies,* pp. 501-530.

Delgado, W. S. a. M., 2009. *Were Russian security services behind the leak of 'Climategate' emails?.* [Online] Available at: http://www.ecoearth.info/shared/reader/welcome.aspx?linkid=144998 [Accessed 3 December 2014].

Denning, D. E., 1999. *Information Warfare and Security.* Boston: Addison-Wesley.

Denning, D. E., 2001. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *Networks and netwars: The future of terror, crime, and militancy,* pp. 239-288.

Disarmament, n.d. *Developments in the field of information and telecommunications in the context of international security.* Geneva: United Nations Publications.

Dowdall, J., 2001. *Controlling the Internet: Balancing limits with guarantees of citizens' freedoms,* Brussels: Security & Defense Agenda.

Dunn, A., 2011. *Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising.* [Online] Available at: http://www.fletcherforum.org/2011/05/15/dunn/ [Accessed 3 December 2014].

Emigh, J., 2010. *RIM vs. India and Saudi Arabia: Let's Make a Deal on Encrypted Data.* [Online] Available at: http://www.brighthand.com/news/rim-vs-india-and-saudi-arabia-lets-make-a-deal-on-encrypted-data/ [Accessed 3 December 2014].

Farivar, C., 2009. *A Brief Examination of Media Coverage of Cyberattacks (2007 - Present)..* s.l.:s.n.

Farnsworth, T., 2013. *Group Coalesces on Cyberspace.* [Online] Available at: http://www.armscontrol.org/act/2013_0708/Expert-Group-Coalesces-on-Cyberspace [Accessed 3 December 2014].

Geers, K., 2014. Pandemonium: Nation States, National Security, and the Internet. *The Tallin Papers,* 1(1), p. 17.

Gellman, B., 2013. *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program.* [Online] Available at: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [Accessed 3 December 2014].

Gerth, J., 1999. *1998 Report told of Lab Breaches and China Threat.* [Online] Available at: http://www.nytimes.com/1999/05/02/world/1998-report-told-of-lab-breaches-and-china-threat.html [Accessed 3 December 2014].

Gertz, B., 2013. *Dam! Sensitive Army database of U.S. dams compromised; Chinese hackers suspected.* [Online] Available at: http://www.washingtontimes.com/news/2013/may/1/sensitive-army-database-us-dams-compromised-chines/?page=all [Accessed 3 December 2014].

Gibson, W., 1984. *Neuromancer.* s.l.:Ace.

Gilpin, R., 1975. *US Power and the Multinational Corporation: The Political Economy of Foreign Direct.* New York: Basic Books.

Gilpin, R., 1981. *War and Change in World Politics.* New York: Cambridge University Press.

Glenny, M., 2010. *States embark on a scramble for cyberspace.* [Online] Available at: http://www.ft.com/intl/cms/s/0/05be0df8-3205-11df-a8d1-00144feabdc0.html#axzz3EhAbeCd7 [Accessed 3 December 2014].

Goldstein, B., 2003. "Imitation in International Relations: Analogies, Vicarious Learning, and Foreign Policy. *International Interactions 29,* pp. 237-267.

Goodin, D., 2012. *Crypto breakthrough shows Flame was designed by world-class scientists.* [Online] Available at: http://arstechnica.com/security/2012/06/flame-crypto-breakthrough/ [Accessed 3 December 2014].

Gorman, S., 2013. *Iran Hacks Energy Firms, U.S. Says.* [Online] Available at: http://online.wsj.com/news/articles/SB10001424127887323336104578501601108021968 [Accessed 3 December 2014].

Gorman, S., 21 April 2009. Computer Spies Breach Fighter-Jet Project. *The Wall Street Journal.*

Gorshenin, V., 2013. *Russia to create cyber-warfare units.* [Online] Available at: http://english.pravda.ru/russia/politics/29-08-2013/125531-cyber_warfare-0/ [Accessed 3 December 2014].

Greenwald, G., 2013. *Obama orders US to draw up overseas target list for cyber-attacks.* [Online] Available at: http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas [Accessed 3 December 2014].

Gross, M. J., 2011. *Enter the Cyber-dragon.* [Online] Available at: http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109 [Accessed 3 December 2014].

Harris, P., 2013. *White House warns of cyber threat from 'aggressive' China and Russia.* [Online] Available at: http://www.theguardian.com/technology/2013/feb/21/white-house-cyber-threat-russia-china [Accessed 3 December 2014].

Hayward, C. R., 2000. *De-Facing Power.* Cambridge: Cambridge University Press.

Heacock, R., 2009. *China shuts down Internet in Xinjiang region after riots.* [Online] Available at: https://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots [Accessed 3 December 2014].

Herz, J. H., 1950. Idealist Internationalism and the Security Dilemma. *World Politics 2,* pp. 157-80.

Hille, K., 2013. *China claims 'mountains of data' on cyber attacks by US.* [Online] Available at: http://www.ft.com/intl/cms/s/0/921f47cc-cdce-11e2-a13e-00144feab7de.html#axzz3EhAbeCd7 [Accessed 3 December 2014].

Hoskins, A., 2010. *War and Media.* s.l.:Polity.

Hughes, R., 2010. A treaty for cyberspace. *International Affairs 86,* pp. 523-541.

Hurwitz, R., May 2012. *Cyber Norms Workshop.* Toronto, Canada Centre, Munk School of Global Affairs.

Ingersoll, G., 2013. *Russia Turns To Typewriters To Protect Against Cyber Espionage.* [Online] Available at: http://www.businessinsider.com/russia-turns-to-typewriters-for-secrets-2013-7 [Accessed 3 December 2014].

Jervis, R., 1978. Cooperation Under the Security Dilemma. *World Politics,* pp. 167-214.

Kagan, D., 1969. *The Outbreak of the Peloponnesian War.* Ithaca: Cornell University Press.

Kalathil, S., 2003. *Open Networks Closed Regimes.* Washington DC: Carnegie Endowment for International Peace.

Keohane, R. O., 1986. Theory of World Politics: Structural Realism and Beyond. In: *Neorealism and Its Critics.* New York: Columbia University Press, pp. 158-203.

Klimburg, A., 2011. Mobilising Cyber Power. Survival. pp. 41-60.

Kramer, F. D., 2009. *Cyberpower and National Security (National Defense University).* First Edition ed. Washington DC: Potomac Books Inc.

Kuehl, D. T., 2009. From Cyberspace to Cyberpower: Defining the Problem. In: F. D. Kramer, ed. *Cyberpower and National Security.* Washington, D.C: Potamac Books, Inc., pp. 24-43.

Lamy, S. L., 2001. Contemporary mainstream approaches: neo-realism and neo-liberalism. In: *The Globalization of World Politics.* New York: Oxford University Press, p. 183.

Langner, R., March 2011. *Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon - TED talk.* [Online] Available at: http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon [Accessed 3 December 2014].

Lasswell, H. D. a. K. A., 1950. *Power and Society: A Framework for Political Inquiry.* New Haven: Yale University Press.

Lawrence, D., 2014. *The U.S. Government Wants 6,000 New 'Cyberwarriors' by 2016.* [Online] Available at: http://www.businessweek.com/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete [Accessed 3 December 2014].

Lemos, R., 2011. *Stuxnet attack more effective than bombs.* [Online] Available at: http://www.infoworld.com/article/2625351/malware/stuxnet-attack-more-effective-than-bombs.html [Accessed 3 December 2014].

Lewis, J., 2013. *Conflict and Negotiation in Cyberspace,* Washington DC: Center for Strategic and International Studies.

Lewis, J. A., 2010. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs,* pp. 55-67.

Lukes, S., 2nd edition. *Power: A Radical View.* London: Palgrave.

Lynn, W., 2010. *Defending a New Domain.* [Online] Available at: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain [Accessed 3 December 2014].

Markoff, J., 2008. *Before the Gunfire, Cyberattacks.* [Online] Available at: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0 [Accessed 3 December 2014].

Markoff, J., 2009. *U.S. and Russia Differ on a Treaty for Cyberspace.* [Online] Available at: http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all&_r=0 [Accessed 3 December 2014].

McCullagh, D., 2007. *FBI turns to broad new wiretap method.* [Online] Available at: http://news.cnet.com/FBIturns-to-broad-new-wiretap-method/2100-7348_3-6154457.html [Accessed 3 December 2014].

Mearsheimer, J. J., 2001. *The Tragedy of Great Power Politics.* New York: W.W. Norton.

Meyer, J., 2013. *"We hack everyone everywhere"—What the NSA whistleblower reveals about the agency's activities abroad.* [Online] Available at: http://finance.yahoo.com/news/hack-everyone-everywhere-nsa-whistleblower-000644289.html [Accessed 3 December 2014].

Moravcsik, A., 1997. Taking Preferences Seriously: A Liberal Theory of International Politics. *International Organization* , p. 513.

Morgenthau, H. J., 1946. *Scientific Man vs. Power Politics.*. Chicago: s.n.

Morgenthau, H. J., 1960. *Politics Among Nations: The Struggle for Power and Peace.* New York: Alfred A. Knopf.

Nakashima, E., 2010. Pentagon's Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Policies. *Washington Post*, 19 March.

Nye, J., 2004b. *Soft Power: The Means to Success in World Politics.* New York: Public Affairs Press.

Nye, J. J., 2004. *Power in the Global Information Age: From Realism to Globalization.* s.l.:Routledge.

ONI, 2004. *A starting point: legal implications of internet filtering,* Toronto: OpenNet Initiative.

Paganini, P., 2012. *Nation state sponsored attacks: the offensive of Governments in cyberspace.* [Online] Available at: http://securityaffairs.co/wordpress/10203/security/nation-state-sponsored-attacks-the-offensive-of-governments-in-cyberspace.html [Accessed 3 December 2014].

Paganini, P., 2014. *$5 Billion in Military Cyber Spending fivefold increase over last year.* [Online] Available at: http://securityaffairs.co/wordpress/22952/cyber-warfare-2/5-billion-military-cyber-spending.html [Accessed 3 December 2014].

Perlroth, N., 2012. *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back.* [Online] Available at: http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all [Accessed 3 December 2014].

Perlroth, N., 2013. *Washington Post Joins List of News Media Hacked by the Chinese.* [Online] Available at: http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html?_r=0 [Accessed 3 December 2014].

Radu, R., 2012. *Negotiating Meanings for Security in the Cyberspace.* Baku, s.n.

Rapoza, K., 2013. *U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press.* [Online] Available at: http://www.forbes.com/sites/kenrapoza/2013/06/22/u-s-hacked-china-universities-mobile-phones-snowden-tells-china-press/ [Accessed 3 December 2014].

Rattray, G., 2009. An Environmental Approach to Understanding Cyberpower. In: *Cyberpower and National Security* . Washington: National Defense University Press, pp. 253-274.

Reardon, R., 2012. *The Role of Cyberspace in International Relations,* San Diego: The MIT Press.

Rohozinski, R., 2008b. Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet. In: *Access Denied: The Practice and Policy of Global Internet Filtering.* s.l.:s.n.

Roscini, M., 2014. *Cyber Operations and Use of Force in International Law*. 1 ed. Oxford: Oxford University Press.

Rosenbaum, R., 2012. *Richard Clarke on Who Was Behind the Stuxnet Attack.* [Online] Available at: http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/?no-ist [Accessed 3 December 2014].

Ryan, J., 2011. *US Official Singles Out China, Russia on Cyber-Spying.* [Online] Available at: http://abcnews.go.com/blogs/politics/2011/11/u-s-takes-hard-line-on-chinese-economic-cyberspying/ [Accessed 3 December 2014].

Samson, T., 2014. *Cyberspying tool could have US, British origins.* [Online] Available at: http://www.dailymail.co.uk/wires/afp/article-2847141/Russia-Saudi-Arabia-main-targets-new-Stuxnet-malware.html [Accessed 3 December 2014].

Sanger, D., 2013. *Confront and Conceal: Obama's secret wars.* s.l.:NOREF Book Review.

Shackelford, S. J., 2014. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace.* s.l.:Cambridge University Press.

Singh, H., 2010. *Spy Game: India readies cyber army to hack into hostile nations' computer systems.* [Online] Available at: http://articles.economictimes.indiatimes.com/2010-08-06/news/27590170_1_computer-systems-spy-game-hackers [Accessed 3 December 2014].

Smith, G., 2010. *'Hacking Back' Could Deter Chinese Cyberattacks, Report Says.* [Online] Available at: http://www.huffingtonpost.com/2013/05/22/hacking-back-chinese-cyberattacks_n_3322247.html [Accessed 3 December 2014].

Stang, G., 2013. Global commons: Between cooperation and competition. *European Union Institute for Security Studies,* pp. 1-4.

Stelter, B., 2009. *Web Pries Lid of Iranian Censorship.* [Online] Available at: http://www.nytimes.com/2009/06/23/world/middleeast/23censor.html [Accessed 3 December 2014].

Stewart, W., 2009. *Were Russian security services behind the leak of 'Climategate' emails?.* [Online] Available at: http://www.dailymail.co.uk/news/article-1233562/Emails-rocked-climate-change-campaign-leaked-Siberian-closed-city-university-built-KGB.html [Accessed 3 December 2014].

Symantec, 2011. *Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually.* [Online] Available at: http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 [Accessed 3 December 2014].

Symantec, 2014. Regin: Top-tier espionage tool enables stealthy surveillance. *Security Response,* 24 November, p. 22.

Tikk, E., 2010. *International Cyber Incidents: Legal Considerations.* Tallin: Cooperative Cyber Defence Centre of Excellence.

UN, 2011. *Report A/65/201 on Developments in the Field of Information and Telecommunications in the Context of International Security .,* s.l.: United Nations.

Ustinova, A., 2010. *Microsoft Says 12th Alleged Russian Spy Was Employee.* [Online] Available at: http://www.bloomberg.com/news/2010-07-14/microsoft-says-12th-alleged-russian-spy-worked-at-its-redmond-headquarters.html [Accessed 3 December 2014].

Villeneuve, N., 2006. *The Filtering Matrix: Integrated Mechanisms of Information Control and the demarcation of borders in cyberspace.* [Online] Available at: http://ojs-prod-lib.cc.uic.edu/ojs/index.php/fm/article/view/1307/1227#author [Accessed 3 December 2014].

Voigt, K., 2011. *Analysis: The hidden cost of cybercrime.* [Online] Available at: http://edition.cnn.com/2011/BUSINESS/06/06/cybercrime.cost/ [Accessed 3 December 2014].

Voß, O., 2011. *Wirtschafts Woche.* [Online] Available at: http://www.wiwo.de/technologie/digitale-welt/ueberwachungs-software-auf-der-spur-des-trojaners/5756462.html [Accessed 3 December 2014].

Wagstaff, J., 30 April, 2001. The Internet Could Be the Site of the Next China-U.S. Standoff. *The Wall Street Journal.*

Walker, D., 2013. *Hacktivists plan to resume DDoS campaign against U.S. banks.* [Online] Available at: http://www.scmagazine.com/hacktivists-plan-to-resume-ddos-campaign-against-us-banks/article/283474/ [Accessed 3 December 2014].

Waltz, K. N., 1946. *Man, The State, and War.* New York: Columbia University.

Waltz, K. N., 1979. *Theory of International Politics.* London: Addison-Wesley.

Waltz, K. N., 1986. 'Reflections on Theory of International Politics: A Response to My Critics', in Robert O. Keohane (ed.), Neorealism and Its Critics. *Columbia University Press,* pp. 322-45.

Weber, M., 1948. Class, Status, Party. In: *From Max Weber: Essays in Sociology.* London: Routledge and Kegan Paul, p. 180.

Wendt, A., 1992. Anarchy is what states make of it: social construction of power politics.. *International Organization,* pp. 392-445.

Wendt, A., 1999. *Social Theory of International Politics.* Cambridge: Cambridge University Press.

Winter, M., 2013. *USA Today.* [Online] Available at: http://www.usatoday.com/story/news/nation/2013/09/05/nsa-snowden-encryption-cracked/2772721/ [Accessed 3 December 2014].

Yannakogeorgos, P., 2013. *Conflict and Cooperation in Cyberspace: The Challenge to National Security.* s.l.:CRC Press.

Ziolkowski, K., 2013. *Peacetime Regime for State Activities in Cyberspace.* Tallinn: NATO CCD COE Publication.

Zittrain, J., 2003. *Empirical Analysis of Internet Filtering in China.* [Online] Available at: http://cyber.law.harvard.edu/wg_home/uploads/203/2003-02.pdf [Accessed 3 December 2014].